



Documentation du logiciel StorageGRID 12.1

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid/index.html> on July 22, 2026.
Always check docs.netapp.com for the latest.

Sommaire

Documentation du logiciel StorageGRID 12.1	1
Découvrez le matériel des appliances StorageGRID	2
Notes de mise à jour	3
Nouveautés de StorageGRID 12.1	3
Capacité	3
Contrôle d'accès	3
Fédération	3
Facilité de gestion	3
S3	4
Sécurité	4
Locataires	5
Mise à niveau	5
Interface utilisateur	5
Fonctionnalités et capacités supprimées ou obsolètes dans StorageGRID	6
Définitions	6
Fin de prise en charge des fonctionnalités StorageGRID	6
Modifications apportées à l'API de gestion de la grille dans StorageGRID	8
Nouveaux points de terminaison pour la modification du mot de passe BMC et des paramètres IP	
LAN	8
Modifications apportées à l'API de gestion des locataires dans StorageGRID	9
Nouvelle API pour la réplification d'objets	9
Modifications apportées à la prise en charge de l'API REST S3 de StorageGRID	9
Lancez-vous avec un système StorageGRID	14
Découvrez StorageGRID	14
Qu'est-ce que StorageGRID ?	14
Clouds hybrides avec StorageGRID	16
Architecture StorageGRID et topologie réseau	17
Grid, nœuds et services	20
La gestion des données par StorageGRID	33
Découvrez StorageGRID	45
Instructions de mise en réseau	53
Directives de mise en réseau pour StorageGRID	53
Types de réseau StorageGRID	54
Exemples de topologie réseau	58
Exigences réseau pour StorageGRID	64
Exigences spécifiques au réseau pour StorageGRID	66
Considérations relatives au réseau propres au déploiement	68
Installation et mise en service du réseau pour StorageGRID	71
Consignes de post-installation pour StorageGRID	72
Référence du port réseau	72
Démarrage rapide pour StorageGRID	82
Installer, mettez à niveau et correctif StorageGRID	86
Installer les nœuds StorageGRID	86

Découvrez le matériel des appliances StorageGRID	86
Installation des nœuds basés sur logiciel	86
Configurer la grille et terminer l'installation	184
Découvrez les étapes obligatoires et facultatives après l'installation de StorageGRID	198
Mettez à niveau le logiciel StorageGRID	199
Mettez à niveau le logiciel StorageGRID	199
Planifiez et préparez la mise à niveau	199
Mise à niveau du logiciel	206
Résoudre les problèmes de mise à niveau de StorageGRID	221
Appliquez le correctif StorageGRID	224
Procédure de correctif StorageGRID	224
Comment StorageGRID est affecté lorsque vous appliquez un correctif	225
Obtenez les matériaux nécessaires pour un correctif StorageGRID	226
Télécharger un fichier correctif StorageGRID	227
Vérifiez l'état du système avant d'appliquer un correctif StorageGRID	228
Appliquer un correctif dans StorageGRID	228
Configuration et gestion d'un système StorageGRID	233
Administrer StorageGRID	233
Démarrage rapide pour l'administration de StorageGRID	233
Lancez-vous avec Grid Manager	234
Contrôle de l'accès à StorageGRID	261
Utiliser la fédération de grille	335
Gérer la sécurité	385
Gérer les locataires	457
Configurer les connexions client	477
Gestion des réseaux et des connexions	522
Gérer des nœuds de stockage	542
Gérer les nœuds d'administration	557
Gestion des objets avec ILM	558
Gérez les objets avec ILM dans StorageGRID	558
ILM et cycle de vie des objets	559
Créez et attribuez des niveaux de stockage dans StorageGRID	582
Utiliser des pools de stockage	584
Utilisation des pools de stockage cloud	592
Gérez les profils de code d'effacement dans StorageGRID	613
Configurer les régions S3 pour StorageGRID	616
Création d'une règle ILM	618
Gestion des règles ILM	636
Travaillez avec les règles ILM et les politiques ILM dans StorageGRID	652
Utilisez le verrouillage d'objet S3	656
Exemples de règles et de règles ILM	665
Renforcement du système pour StorageGRID	687
Découvrez le renforcement du système pour StorageGRID	687
Recommandations de renforcement pour les mises à niveau logicielles StorageGRID	688
Instructions de renforcement des réseaux StorageGRID	689

Instructions de renforcement pour les nœuds StorageGRID	690
Recommandations de renforcement pour TLS et SSH dans StorageGRID	694
Recommandations de renforcement pour les journaux, les mots de passe et les messages d'audit dans StorageGRID	696
StorageGRID avec FabricPool	697
Flux de configuration pour l'utilisation de StorageGRID avec FabricPool	697
Informations nécessaires pour connecter StorageGRID en tant que niveau cloud FabricPool	699
Utilisez l'assistant d'installation FabricPool	700
Configurez StorageGRID manuellement	714
Configurez ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud FabricPool	725
Configurer les entrées du serveur DNS pour StorageGRID avec FabricPool	727
Meilleures pratiques StorageGRID pour FabricPool	727
Supprimez les données FabricPool de StorageGRID	732
Utilisez les locataires et clients StorageGRID	734
Utilisez un compte de locataire	734
Utilisez un compte de locataire StorageGRID	734
Comment se connecter et se déconnecter	735
Tableau de bord Tenant Manager dans StorageGRID	737
API de gestion des locataires	740
Utiliser les connexions de fédération de grille	745
Gestion des groupes et des utilisateurs	755
Gestion des clés d'accès S3	773
Gestion des compartiments S3	778
Gérez les services de la plateforme S3	810
UTILISEZ L'API REST S3	846
Versions et mises à jour prises en charge de l'API REST StorageGRID S3	846
Requêtes S3 API prises en charge dans StorageGRID	850
Tester la configuration de l'API REST S3 de StorageGRID	870
Implémentation de l'API REST S3 par StorageGRID	871
Prise en charge de l'API REST Amazon S3	888
Opérations personnalisées StorageGRID	944
Gérer les politiques d'accès	966
Opérations S3 suivies dans les journaux d'audit de StorageGRID	994
Utilisation de l'API REST Swift (fin de vie)	995
Prise en charge de l'API REST Swift dans StorageGRID	995
Surveillance et dépannage d'un système StorageGRID	996
Surveiller le système StorageGRID	996
Utiliser AutoSupport	996
Surveiller un système StorageGRID	1011
Consultez et gérez le tableau de bord dans StorageGRID	1012
Afficher la page nœuds	1014
Informations à surveiller régulièrement	1044
Gérer les alertes	1072
Référence des fichiers journaux	1109
Configurer la gestion des journaux et le serveur syslog externe	1130

Configurer le serveur de messagerie	1146
Utiliser la surveillance SNMP	1148
Collecte de données StorageGRID supplémentaires	1160
Dépanner le système StorageGRID	1174
Dépanner un système StorageGRID	1174
Résoudre les problèmes liés au stockage et aux objets	1181
Résolvez les problèmes de métadonnées dans StorageGRID	1200
Dépanner les erreurs de certificat dans StorageGRID	1202
Résolvez les problèmes liés au nœud d'administration et à l'interface utilisateur dans StorageGRID	1203
Résolvez les problèmes de réseau, de matériel et de plateforme dans StorageGRID	1207
Dépanner les messages d'erreur du serveur syslog externe pour StorageGRID	1214
Découvrez les problèmes de mise en cache des équilibres de charge dans StorageGRID	1217
Examiner les journaux d'audit	1218
Journaux et messages d'audit	1218
Comment les messages d'audit transitent dans le système StorageGRID jusqu'au fichier audit.log pour conservation.	1219
Accédez aux fichiers du journal des audits depuis la ligne de commandes du nœud d'administration StorageGRID	1222
Découvrez la rotation des fichiers du journal des audits dans StorageGRID	1223
Format du fichier journal d'audit.	1224
Format du message d'audit	1236
Messages d'audit et cycle de vie de l'objet	1241
Messages d'audit	1247
Augmentez la capacité ou les fonctionnalités de votre système StorageGRID	1295
Découvrez comment étendre votre système StorageGRID	1295
Planification de l'expansion	1296
Planification de l'extension des données répliquées dans StorageGRID	1296
Planification de l'extension des données à codage d'effacement (EC) dans StorageGRID	1297
Découvrez le rééquilibrage EC après l'extension de StorageGRID.	1298
directives d'expansion	1302
Instructions pour l'ajout de capacité d'objets dans StorageGRID	1303
Instructions pour l'ajout de capacité de métadonnées dans StorageGRID	1304
Instructions pour l'ajout de nœuds de grille dans StorageGRID	1306
Instructions pour l'ajout d'un nouveau site dans StorageGRID	1307
Préparez-vous à étendre votre système StorageGRID	1308
Téléchargez et extrayez les fichiers d'installation de StorageGRID	1309
Vérification du matériel et de la mise en réseau	1314
Ajout de nœuds grid ou d'un site	1315
Résumé du processus d'ajout de nœuds de grille ou de nouveaux sites à StorageGRID	1315
Ajoutez ou mettez à jour des sous-réseaux au réseau Grid pour l'extension dans StorageGRID.	1316
Déployez de nouveaux nœuds de grille dans StorageGRID	1318
Effectuez une extension StorageGRID	1322
Ajout de volumes de stockage	1327
Ajoutez des volumes de stockage à votre système StorageGRID	1327
Ajoutez des volumes de stockage aux nœuds de stockage VMware dans StorageGRID	1329

Ajoutez des volumes à connexion directe ou SAN aux nœuds de stockage Linux dans StorageGRID	1330
Configuration du système faisant l'objet de l'extension	1334
Configurez les nœuds et sites nouvellement ajoutés dans StorageGRID.	1334
Vérifiez que les nœuds de stockage sont actifs après une extension de StorageGRID	1336
Copiez les métriques Prometheus vers les nouveaux nœuds d'administration dans StorageGRID.	1336
Copiez les journaux d'audit vers les nouveaux nœuds d'administration dans StorageGRID.	1337
Rééquilibrez les données à codage d'effacement après l'ajout de nœuds à votre système StorageGRID.	1339
Résolution des erreurs d'extension dans StorageGRID	1342
Maintenance d'un système StorageGRID	1344
Maintenance du grid StorageGRID	1344
Avant de commencer	1344
Procédures de maintenance des appareils	1344
Téléchargez le package de récupération StorageGRID	1344
Désaffectez les nœuds ou le site	1345
Mettre hors service un nœud ou un site StorageGRID	1345
Désaffectation des nœuds	1345
Désaffecter le site	1363
Renommez la grille, le site ou le nœud	1387
Utilisez la procédure de renommage StorageGRID.	1387
Ajouter ou mettre à jour les noms d'affichage StorageGRID	1391
Procédures de nœud	1397
Procédures de maintenance des nœuds StorageGRID	1397
Déplacer le service ADC dans StorageGRID	1397
Convertir un nœud de stockage StorageGRID en un nœud de données uniquement	1398
Procédures de redémarrage, d'arrêt et d'alimentation.	1400
Procédures de remap de port	1412
Procédures de Server Manager	1416
Procédures réseau	1425
Mise à jour des sous-réseaux pour StorageGRID Grid Network	1425
Configurez les adresses IP	1427
Ajoute des interfaces au nœud existant.	1447
Configurer les serveurs DNS dans StorageGRID	1450
Modifier la configuration DNS pour un nœud StorageGRID unique	1451
Gérer les serveurs NTP dans StorageGRID	1454
Rétablir la connectivité réseau pour les nœuds StorageGRID isolés	1455
Procédures d'hôte et de middleware	1457
Migrer un nœud StorageGRID vers un nouvel hôte Linux.	1457
Configurer une machine virtuelle VMware pour un redémarrage automatique dans StorageGRID	1459
Récupérer ou remplacer des nœuds	1460
Avertissements et considérations pour la récupération des nœuds StorageGRID	1460
Conditions préalables à la récupération des nœuds de la grille	1460
Ordre de restauration de nœud en cas de défaillance d'un serveur hébergeant plusieurs nœuds de la grille	1461
Adresses IP des nœuds restaurés	1461

Rassemblez les matériaux nécessaires pour la récupération des nœuds de la grille StorageGRID.	1461
Téléchargez et extrayez les fichiers d'installation StorageGRID	1462
Sélectionnez la procédure de récupération du nœud StorageGRID	1468
Restaurez les données après une panne de nœud de stockage	1469
Récupérer après des pannes de nœuds de stockage StorageGRID	1469
Restaurez le nœud de stockage de l'appliance	1471
Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact	1485
Restaurez les données après une panne de disque système	1494
Restaurez vos données après une panne de nœud d'administration	1506
Récupération du nœud d'administration principal ou non principal dans StorageGRID	1506
Récupérez après une défaillance du nœud d'administration principal en utilisant le même nœud d'administration principal	1507
Récupérez après des défaillances du nœud d'administration principal à l'aide d'un nœud d'administration non principal	1515
Restaurez vos données en cas de défaillance d'un nœud d'administration non principal	1523
Restaurez les données à partir d'une défaillance de nœud de passerelle	1530
Remplacer le nœud de passerelle StorageGRID	1531
Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle StorageGRID	1531
Échec de la restauration à partir du nœud d'archivage	1532
Récupérer après des pannes de nœuds d'archivage StorageGRID	1532
Remplacez le nœud Linux	1532
Remplacer un nœud Linux dans StorageGRID	1532
Déployer de nouveaux hôtes Linux pour StorageGRID	1533
Restaurez les nœuds StorageGRID sur l'hôte	1534
Effectuez des étapes de récupération supplémentaires du nœud StorageGRID	1539
Remplacez un nœud VMware dans StorageGRID par un nœud de récupération	1540
Remplacez le nœud VMware dans StorageGRID par SG1000 ou SG100	1541
Étape 1 : Remplacez le nœud VMware	1542
Étape 2 : Terminez la récupération du nœud	1547
Remplacez le nœud défectueux par l'appliance de services	1547
Remplacez le nœud StorageGRID défaillant par un dispositif de services	1547
Installer l'appliance de services StorageGRID (changement de plateforme uniquement)	1548
Préparez l'appliance StorageGRID pour la réinstallation (remplacement de la plateforme uniquement)	1548
Démarez l'installation du logiciel StorageGRID sur un appareil de services	1549
Surveillez l'installation de l'appliance de services StorageGRID	1551
Comment le support technique récupère un site StorageGRID	1553
Solutions et ressources StorageGRID	1555
Comment gérer StorageGRID à l'aide de la console NetApp	1556
Mentions légales	1557
Droits d'auteur	1557
Marques déposées	1557
Brevets	1557
Politique de confidentialité	1557
Licence API	1557
Source ouverte	1557

Documentation du logiciel StorageGRID 12.1

Découvrez le matériel des appliances StorageGRID

Accédez à "[Documentation de l'appliance StorageGRID](#)" pour savoir comment installer, configurer et maintenir les appliances de stockage et de services StorageGRID.

Notes de mise à jour

Nouveautés de StorageGRID 12.1

StorageGRID 12.1 introduit les fonctionnalités et modifications fonctionnelles suivantes.

Pour plus de détails sur les problèmes résolus et les problèmes connus dans les versions récentes de StorageGRID 12.1, consultez ["Notes de version de StorageGRID 12.1"](#). Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

Capacité

Le rééquilibrage EC utilise désormais l'espace libre

Le rééquilibrage EC utilise désormais l'espace libre au lieu de l'espace utilisé. Voir ["Découvrez le rééquilibrage EC après l'extension de StorageGRID."](#)

Espace autorisé pour les métadonnées

Vous pouvez désormais augmenter la valeur maximale autorisée des métadonnées de 3,96 To à 7,92 To. Reportez-vous à ["Espace de métadonnées autorisé"](#).

Contrôle d'accès

SSO utilisant OIDC

Vous pouvez maintenant ["Configurer l'authentification unique \(SSO\) dans StorageGRID à l'aide d'OpenID Connect \(OIDC\)"](#).

Fédération

Espace de noms global

Vous pouvez désormais configurer un espace de noms global pour permettre aux locataires d'accéder aux compartiments sur plusieurs systèmes StorageGRID. Consultez ["Découvrez l'espace de noms global"](#).

Facilité de gestion

Service ADC à déplacement automatique

["Lorsque cela est nécessaire pour atteindre le quorum de l'ADC"](#), le service ADC sera désormais déplacé automatiquement lorsque vous ["conversion d'un nœud de stockage en nœud de données uniquement"](#) ou ["mise hors service d'un nœud de stockage"](#).

Récupération du nœud d'administration principal

Vous pouvez désormais récupérer n'importe quel nœud à partir d'un nœud d'administration non principal. Consultez ["Récupération après des défaillances du nœud d'administration principal"](#).

S3

Activer le verrouillage d'objets S3 sur les compartiments existants

Lorsque l'option « Autoriser le verrouillage d'objets S3 pour les compartiments existants » est activée, un compte locataire S3 peut désormais activer le verrouillage d'objets S3 pour un compartiment existant. Après qu'un compte locataire S3 a activé le verrouillage d'objets S3 pour un compartiment existant, il ne peut plus être désactivé.

Réplication autorisée pour les compartiments S3 avec Object Lock activé

Vous pouvez désormais utiliser CloudMirror pour répliquer des objets dans des compartiments S3 avec Object Lock activé. Reportez-vous à ["Découvrez les services de plateforme"](#).

Activer la réplication inter-grilles pour les compartiments non vides

Vous pouvez désormais activer la réplication inter-grilles pour les compartiments non vides. Consultez ["Conditions requises pour la réplication entre les grilles"](#).

Opérations par lots S3 (FPVR uniquement)

Vous pouvez utiliser les opérations par lots S3 pour répliquer des objets existants dans un compartiment avec le versionnage activé que vous prévoyez de configurer pour la réplication inter-grilles.

Cette fonctionnalité nécessite l'approbation de FPVR pour StorageGRID 12.1. Pour utiliser cette fonctionnalité, contactez votre représentant commercial.

En-têtes S3 REST API non fonctionnels

Les If-Match et If-None-Match en-têtes sont acceptés mais non fonctionnels pour l'API REST S3 ["PutObject"](#), ["CompleteMultipartUpload"](#), ["Objet de copie"](#) et ["DeleteObject"](#).

Pour plus d'informations, veuillez consulter ["Modifications apportées à la prise en charge de l'API REST S3 de StorageGRID"](#).

Prise en charge des valeurs de somme de contrôle précalculées

L'interface SPI REST S3 prend désormais en charge les valeurs de somme de contrôle précalculées et l'`'x-amz-checksum-type'` en-tête de requête. Reportez-vous à ["Mises à jour de la prise en charge de l'API REST"](#).

Sécurité

Vérification multi-administrateurs

La vérification multi-administrateurs (MAV) contribue à prévenir les modifications accidentelles ou non autorisées de votre système StorageGRID. Consultez ["Découvrez la vérification multi-administrateur de StorageGRID"](#).

Mises à jour de la politique de sécurité pour FIPS

Les critères stricts de la politique FIPS ont été mis à jour. Voir ["Sélectionnez une stratégie de sécurité dans Gérer la stratégie TLS et SSH"](#).

Locataires

Synchronisation des comptes

La fonctionnalité *account clone* fait désormais référence à un clonage unique des informations d'un compte locataire spécifique.

La synchronisation des comptes est une nouvelle fonctionnalité qui vous permet de répliquer automatiquement et en continu les comptes de locataires, les groupes de locataires, les utilisateurs de locataires et les clés d'accès S3 entre les systèmes StorageGRID dans une ou plusieurs connexions de fédération de grilles. Reportez-vous à ["Découvrez la synchronisation des comptes dans StorageGRID"](#).

Points de terminaison Kafka et authentification mTLS

Le protocole Mutual Transport Layer Security (mTLS) est désormais pris en charge pour les points de terminaison Kafka. Consultez ["Configurer les terminaux des services de plateforme"](#).

Nombre maximal de compartiments

Un système StorageGRID prend désormais en charge un maximum de 20 000 compartiments pour chaque compte locataire S3.

Mise à niveau

Le délai d'activation des fonctionnalités est augmenté

Lors de la mise à niveau de StorageGRID vers la version 12.1, le temps d'activation des fonctionnalités est passé de moins de cinq minutes à une heure. Reportez-vous à ["Estimez le temps nécessaire pour effectuer une mise à niveau de StorageGRID"](#).

Interface utilisateur

Page des paramètres BMC

Un nouvel onglet « Paramètres BMC » a été ajouté à la page « Nœuds » dans Grid Manager pour permettre la réinitialisation du mot de passe BMC et la modification des paramètres IP LAN du BMC. Consultez ["Modifier le mot de passe BMC de l'appliance"](#) et ["Modifier les paramètres IP LAN du BMC du nœud de l'appliance"](#). De nouveaux points de terminaison API ont également été ajoutés pour prendre en charge ces fonctions. Consultez ["Nouveaux points de terminaison pour la modification du mot de passe BMC et des paramètres IP LAN"](#).

Notifications par e-mail

Le Gestionnaire de grille dispose désormais d'une page de messagerie commune permettant de configurer et de gérer les notifications par e-mail pour les alertes, AutoSupport et la vérification multi-administrateurs (MAV). Reportez-vous à ["Configurer le serveur de messagerie"](#).

Mise à jour de la page du coût des liens

StorageGRID 12.1 fournit des informations et des paramètres plus détaillés sur les coûts des liens. Consultez ["Gérer les coûts de liaison"](#).

Contrôle du port USB

Vous pouvez désormais activer ou désactiver les ports USB via Grid Manager. Consultez ["Contrôlez l'accès à distance via les ports USB"](#).

Fonctionnalités et capacités supprimées ou obsolètes dans StorageGRID

Découvrez les fonctionnalités et capacités qui ont été supprimées ou rendues obsolètes dans StorageGRID 12.1.0. Avant de procéder à la mise à niveau, vérifiez si des fonctionnalités supprimées ou rendues obsolètes affectent vos applications clientes ou la configuration de votre grid.

Définitions

Obsolète

Vous ne devez pas utiliser cette fonctionnalité dans les nouveaux environnements de production. Les environnements de production existants peuvent continuer à utiliser cette fonctionnalité.

Fin de vie

Dernière version livrée qui prend en charge cette fonctionnalité. Dans certains cas, la documentation de la fonction peut être supprimée à ce stade.

Supprimé

Première version que **ne prend pas** en charge la fonction.

Fin de prise en charge des fonctionnalités StorageGRID

Les fonctions obsolètes seront supprimées dans les versions majeures N+2. Par exemple, si une fonction est obsolète dans la version N (par exemple, 6.3), la dernière version où la fonction existera est N+1 (par exemple, 6.4). La version N+2 (par exemple, 6.5) est la première version lorsque la fonction n'existe pas dans le produit.

Pour plus d'informations, reportez-vous au ["Page de support des versions logicielles"](#).



Dans certains cas, NetApp peut mettre fin à la prise en charge de certaines fonctionnalités plus tôt que prévu.

Fonction	Obsolète	Fin de vie	Supprimé	Liens vers la documentation précédente
Paramètre SSE global pour le chiffrement AES-128	12,1	12,2	12,3	À compter de StorageGRID 12.1.0, la prise en charge du chiffrement AES-128 des nouvelles données d'objet stockées au repos est obsolète. La prise en charge de la récupération des objets stockés initialement chiffrés avec AES-128 est maintenue.
Alarmes, héritées (<i>pas Alertes</i>)	11,7	11,8	11,9	"Référence des alarmes (StorageGRID 11.8)"

Fonction	Obsolète	Fin de vie	Supprimé	Liens vers la documentation précédente
Prise en charge du nœud d'archivage	11,7	11,8	11,9	"Considérations relatives à la désaffectation des nœuds d'archivage (StorageGRID 11.8)" Remarque : avant de commencer votre mise à niveau, vous devez : 1. Mettez hors service tous les nœuds d'archivage. Consultez "Désaffectation du nœud grid (site du doc StorageGRID 11.8)". 2. Supprimez toutes les références aux nœuds d'archivage des pools de stockage et des stratégies ILM. Consultez "Base de connaissances NetApp : guide de résolution des mises à niveau logicielles 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 mise en conteneurs Docker	11,8	11,9	À DÉFINIR	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 "exigences logicielles pour les nœuds basés sur des logiciels" pour une liste des versions de Docker actuellement prises en charge.
Configuration de l'e-mail (ancienne version)	11,9	12,0	12,1	"Configurer les notifications d'alarmes (système hérité) (StorageGRID 11.8)"
Exportation d'audit NFS	11,8	11,9	12,0	"Configuration de l'accès client d'audit pour NFS (StorageGRID 11.8)"
Remappage des ports	12,0	12,1	12,2	
Prise en charge de l'API Swift	11,7	11,9	12,0	"Utiliser l'API REST de Swift (StorageGRID 11.8)"
RHEL 8,8	11,9	11,9	12,0	

Fonction	Obsolète	Fin de vie	Supprimé	Liens vers la documentation précédente
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	

Se reporter également à :

- ["Modifications apportées à l'API de gestion du grid"](#)
- ["Modifications apportées à l'API de gestion des locataires"](#)

Modifications apportées à l'API de gestion de la grille dans StorageGRID

StorageGRID 12.1 utilise la version 4 de l'API de gestion de la grille. La version 4 remplace la version 3 ; toutefois, les versions 1, 2 et 3 restent prises en charge.



Vous pouvez continuer à utiliser les versions obsolètes de l'API de gestion avec StorageGRID ; cependant, 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 12.0 ou une version ultérieure, vous pouvez désactiver les API obsolètes en utilisant l'`PUT /grid/config/management`API.

Pour en savoir plus, rendez-vous sur ["Utilisez l'API de gestion du grid"](#).

Nouveaux points de terminaison pour la modification du mot de passe BMC et des paramètres IP LAN

Le point de terminaison suivant a été ajouté pour vous permettre de ["modifier le mot de passe BMC d'un appareil"](#).

```
PUT /bmc-configuration/root-password
```

Les points de terminaison suivants ont été ajoutés pour vous permettre de ["modifier ou afficher les paramètres IP LAN du BMC"](#).

```
PUT /grid/bmc/{node-id}/lan-ip-config
```

```
GET /grid/bmc/{node-id}/lan-ip-config
```

Modifications apportées à l'API de gestion des locataires dans StorageGRID

StorageGRID 12.1 utilise la version 4 de l'API de gestion des locataires. La version 4 remplace la version 3 ; toutefois, les versions 1, 2 et 3 restent prises en charge.



Vous pouvez continuer à utiliser les versions obsolètes de l'API de gestion des locataires avec StorageGRID ; toutefois, la prise en charge de ces versions de l'API sera supprimée dans une prochaine version de StorageGRID. Après la mise à niveau vers StorageGRID 12.0 ou une version ultérieure, vous pouvez désactiver les API obsolètes à l'aide de l' `PUT /grid/config/management API`.

Pour en savoir plus, rendez-vous sur ["Découvrez l'API de gestion des locataires"](#).

Nouvelle API pour la réplication d'objets

Vous pouvez utiliser le `/org/cross-grid-replication/{versionId}/replicate` API pour répliquer manuellement des objets sur un bucket existant dont la réplication inter-grille est nouvellement configurée.

Modifications apportées à la prise en charge de l'API REST S3 de StorageGRID

L'API REST S3 utilisée par StorageGRID est mise à jour régulièrement.

Relâchez	Commentaires
12.1.0	• <code>If-Match</code> L' <code>If-Match</code> en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut renvoyer un message d'erreur (501 Not Implemented). Si l' <code>If-Match</code> en-tête est accepté mais non fonctionnel, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict. • <code>If-None-Match</code> L' <code>If-None-Match</code> en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut entraîner un message d'erreur (501 Not Implemented). Si l' <code>If-None-Match</code> en-tête est accepté mais non fonctionnel, une alerte peut s'afficher avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict. • Ajout de la prise en charge des valeurs de somme de contrôle précalculées pour les requêtes et en-têtes suivants : ◦ <code>CompleteMultipartUpload</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, et <code>x-amz-checksum-crc64nvme</code> ◦ <code>CreateMultipartUpload</code>: <code>CRC32</code>, <code>CRC32C</code> et <code>CRC64NVME</code> pour <code>x-amz-checksum-algorithm</code> ◦ <code>CopyObject</code>: <code>CRC32</code>, <code>CRC32C</code>, <code>CRC64NVME</code>, et <code>SHA256</code> pour <code>x-amz-checksum-algorithm</code> ◦ <code>PutObject</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code> et <code>x-amz-checksum-crc64nvme</code> ◦ <code>UploadPart</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code> et <code>x-amz-checksum-crc64nvme</code> • Ajout de la prise en charge de <code>x-amz-checksum-type</code> pour <code>CreateMultipartUpload</code> et <code>CompleteMultipartUpload</code>. • Ajout de la prise en charge de la clé de condition de stratégie <code>s3:x-amz-copy-source</code>. • Autoriser l'activation du verrouillage d'objets S3 sur les compartiments existants.
12,0	• Ajout de la prise en charge du partage de ressources inter-origines (CORS) pour une interface de gestion, qui permet à un autre domaine d'accéder aux données dans StorageGRID à l'aide des API de gestion. "En savoir plus >>" . • Ajout de la prise en charge de STS AssumeRole et de la stratégie de session. Voir "un exemple de politique de session". Vous pouvez configurer AssumeRole dans les groupes de locataires.

Relâchez	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 pré-calculées pour les demandes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonction pour vérifier l'intégrité des objets téléchargés : ◦ Téléchargement CompleteMultipartUpload : x-amz-checksum-sha256 ◦ CreateMultipartUpload : x-amz-checksum-algorithm ◦ GetObject : x-amz-checksum-mode ◦ Objet principal : x-amz-checksum-mode ◦ ListParts ◦ PutObject : x-amz-checksum-sha256 ◦ UploadPart : x-amz-checksum-sha256 • Ajout de la possibilité pour l'administrateur du grid 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 compartiment et mode de conservation des objets : gouvernance ou conformité, si l'administrateur du grid l'autorise. ◦ La période de conservation par défaut du compartiment et la date de conservation de l'objet jusqu'au : doivent être inférieures ou égales à ce qui est autorisé par la période de conservation maximale définie par l'administrateur du grid. • Meilleure prise en charge de aws-chunked l'encodage de contenu et des valeurs de diffusion en continu x-amz-content-sha256. Limites : ◦ Le cas échéant, chunk-signature est facultatif et non validé ◦ S'il est présent, x-amz-trailer le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour qu'ils correspondent aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service" .
11,7	• Ajouté "Référence rapide : demandes d'API S3 prises en charge". • Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge de l'en-TÊTE de réponse spécifique à StorageGRID x-ntap-sg-cgr-replication-status pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grid. • Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.

Relâchez	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes GET Object et HEAD Object. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. • Ajout de la prise en charge de la <code>s3:object-lock-remaining-retention-days</code> clé de condition de règle pour définir la plage de périodes de conservation autorisées pour vos objets. • Modification de la taille <i>recommandée</i> maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
11,5	• Ajout de la prise en charge de la gestion du chiffrement de compartiment. • Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. • L' `Content-MD5` en-tête de la demande est désormais correctement pris en charge.
11,4	• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge. • Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. • Prise en charge supplémentaire des notifications de compartiment pour le <code>s3:ObjectRestore:Post</code> type d'événement. • Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Prise en charge supplémentaire des opérations de SUPPRESSION, d'OBTENTION et de MISE du cycle de vie du compartiment (action d'expiration uniquement) et de <code>x-amz-expiration</code> l'en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Relâchez	Commentaires
11,2	Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge. Remarque : les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.
11,0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout de la prise en charge des contraintes d'emplacement du balisage d'objets pour les compartiments, ainsi que de la cohérence disponible.
10,4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour la gestion des versions.
10,2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10,1	Ajout de la prise en charge du téléchargement en plusieurs parties, des requêtes de type hébergement virtuel et de l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID . La version actuellement prise en charge de la <i>Référence API du service de stockage simple</i> est 2006-03-01.

Consultez "[Versions et mises à jour prises en charge de l'API REST S3](#)" pour plus d'informations.

Lancez-vous avec un système StorageGRID

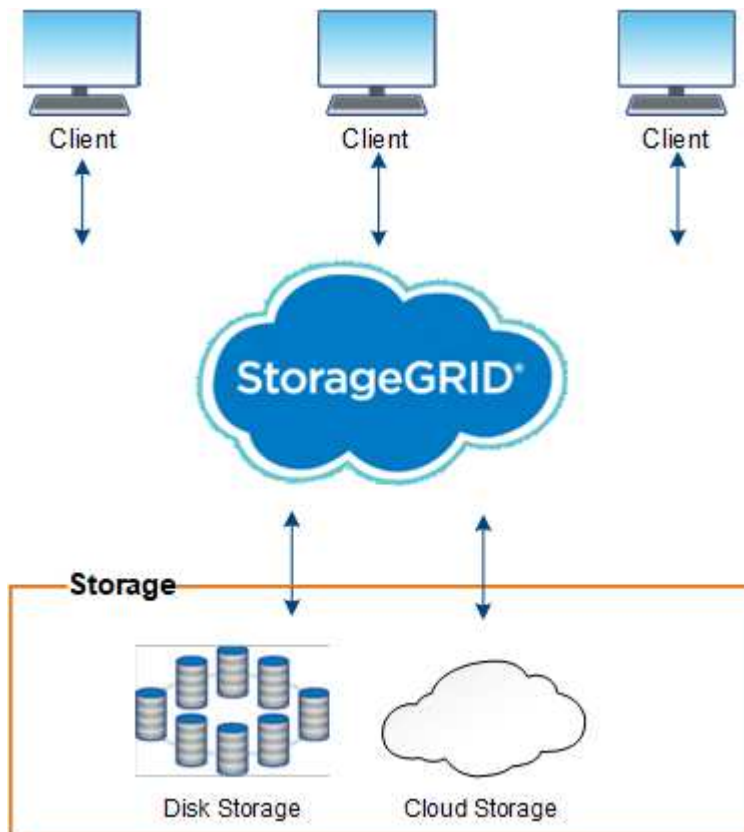
Découvrez StorageGRID

Qu'est-ce que StorageGRID ?

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

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

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



La prise en charge des nœuds d'archivage a été supprimée. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe via l'API S3 a été remplacé par "[Pools de stockage cloud ILM](#)", qui offre davantage de fonctionnalités.

Avantages de StorageGRID

La baie StorageGRID présente plusieurs avantages :

- Référentiel de données distribué géographiquement extrêmement évolutif et facile à utiliser pour les données non structurées.
- Le protocole de stockage d'objets standard Amazon Web Services Simple Storage Service (S3).
- Compatibilité avec le cloud hybride. La gestion du cycle de vie des informations basée sur des règles stocke les objets dans des clouds publics, notamment Amazon Web Services (AWS) et Microsoft Azure. Les services de plateforme StorageGRID permettent la réplication de contenu, la notification d'événements et la recherche de métadonnées d'objets stockés dans les clouds publics.
- Protection flexible des données pour assurer la durabilité et la disponibilité. Les données peuvent être protégées au moyen de la réplication et du code d'effacement à plusieurs couches. La vérification des données au repos et à la volée garantit l'intégrité des données conservées à long terme.
- Gestion dynamique du cycle de vie des données pour vous aider à gérer les coûts de stockage. Vous pouvez créer des règles ILM pour gérer le cycle de vie des données au niveau objet, personnaliser la localisation des données, la durabilité, les performances, le coût et de conservation des données.
- Haute disponibilité du stockage de données et certaines fonctions de gestion, avec équilibrage de la charge intégré pour optimiser la charge de données sur les ressources StorageGRID.
- Prise en charge de plusieurs comptes de locataires de stockage pour isoler les objets stockés sur votre système par des entités différentes.
- De nombreux outils de contrôle de l'état de santé de votre système StorageGRID, notamment un système d'alertes complet, un tableau de bord graphique et des États détaillés pour tous les nœuds et sites.
- Prise en charge du déploiement logiciel ou matériel. Vous pouvez déployer StorageGRID sur l'une des plateformes suivantes :
 - Ordinateurs virtuels exécutés dans VMware.
 - Moteurs de mise en conteneurs sur hôtes Linux.
 - Appareils conçus par StorageGRID.
 - Les appliances de stockage fournissent le stockage objet.
 - Les appliances de services proposent des services d'administration du grid et d'équilibrage de la charge.
- Conformité avec les exigences pertinentes de ces réglementations en matière de stockage :
 - Securities and Exchange Commission (SEC), in 17 CFR § 240.17a-4(f), qui réglemente les membres, courtiers ou courtiers en bourse.
 - Autorité de réglementation du secteur financier (FINRA) règle 4511(c) qui diffère du format et des exigences médias de la règle SEC 17a-4(f).
 - La Commodity futures Trading Commission (CFTC) dans le règlement 17 CFR § 1.31(c)-(d), qui réglemente la négociation des marchandises à terme.
- Les opérations de mise à niveau et de maintenance sans interruption. Maintenez l'accès au contenu lors des procédures de mise à niveau, d'extension, de déclasserment et de maintenance.
- Gestion fédérée des identités. 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 du protocole Security Assertion Markup Language 2.0 (SAML 2.0) ou OpenID Connect (OIDC) pour l'échange de données d'authentification et d'autorisation entre StorageGRID et un fournisseur d'identité externe tel que Active Directory Federation Services (AD FS).

Clouds hybrides avec StorageGRID

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

Pools de stockage cloud

Les pools de stockage cloud vous permettent de stocker des objets en dehors du système StorageGRID. Par exemple, vous pourriez vouloir déplacer des objets rarement consultés vers un stockage cloud à moindre coût, comme Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le niveau d'accès Archive dans Microsoft Azure Blob Storage. Ou, vous pourriez vouloir maintenir une sauvegarde cloud des objets StorageGRID, qui peut être utilisée pour récupérer des données perdues à la suite 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 ajoutée pour extraire un objet de la cible du pool de stockage cloud.

Services de plateforme S3

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

- Le service de réplication CloudMirror met automatiquement en miroir les objets spécifiés dans un compartiment S3 cible, qui peut se trouver sur Amazon S3 ou sur un second système StorageGRID.
- Le service de notification d'événements envoie des messages 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 les métadonnées des objets à un service Elasticsearch externe, permettant ainsi de rechercher, visualiser et analyser ces métadonnées à l'aide d'outils tiers.

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

Tiering des données ONTAP avec FabricPool

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

Contrairement aux solutions de hiérarchisation manuelle, FabricPool réduit le 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 associées

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

- ["Gestion des services de plateforme"](#)
- ["Configuration de StorageGRID pour FabricPool"](#)

Architecture StorageGRID et topologie réseau

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

En savoir plus sur le ["types de nœuds de grille"](#) .

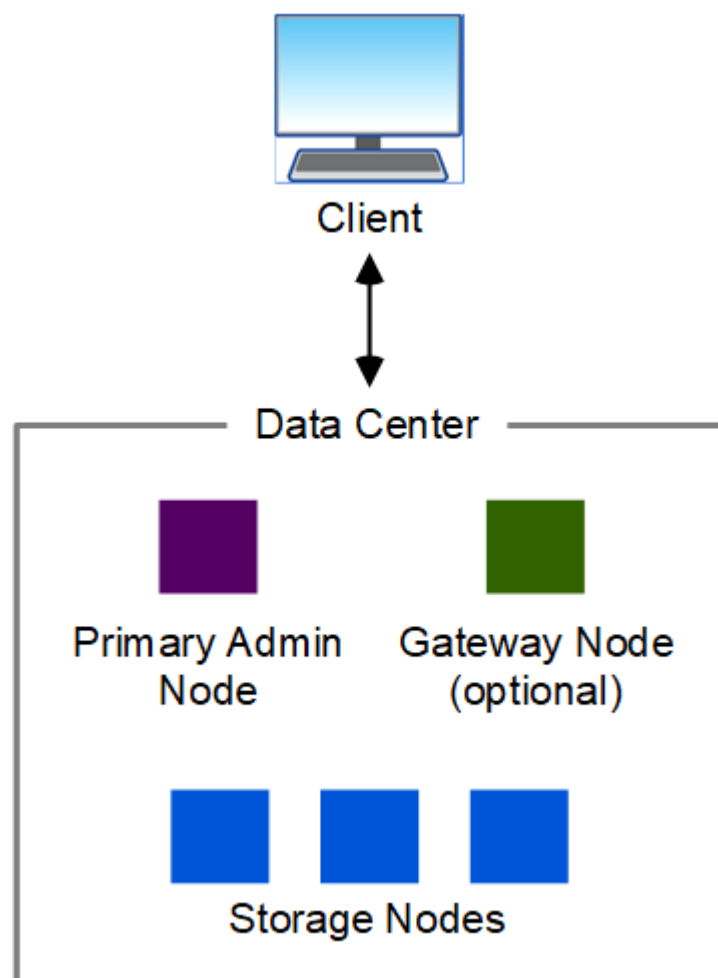
Pour plus d'informations sur la topologie du réseau StorageGRID, les exigences et les communications de la grille, veuillez consulter ["Instructions de mise en réseau"](#).

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. Le nombre maximal de sites par déploiement est de 16.

Sur un seul site

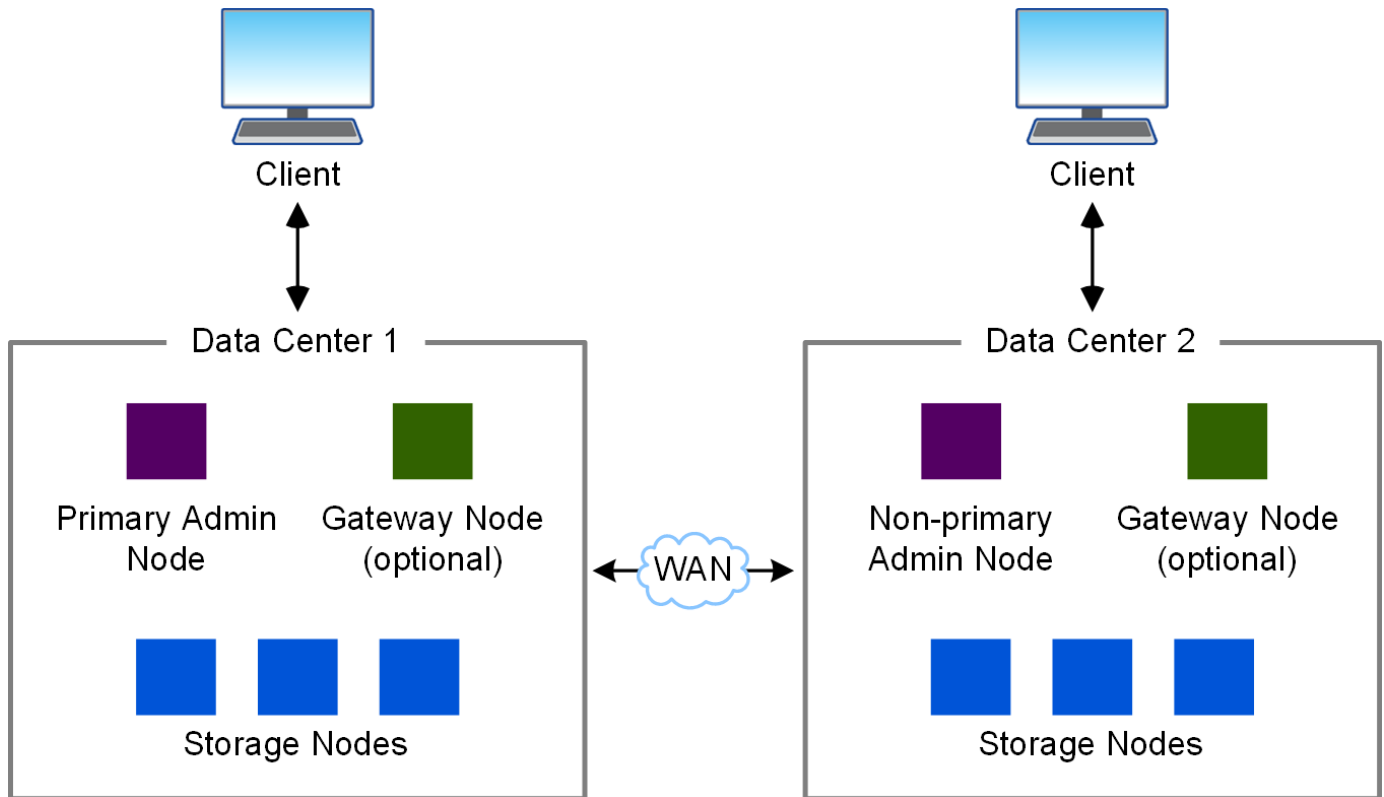
Dans un déploiement avec un site unique, l'infrastructure et les opérations du système StorageGRID sont centralisées.



Sites multiples

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

Les sites sont souvent situés dans des endroits géographiquement 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.



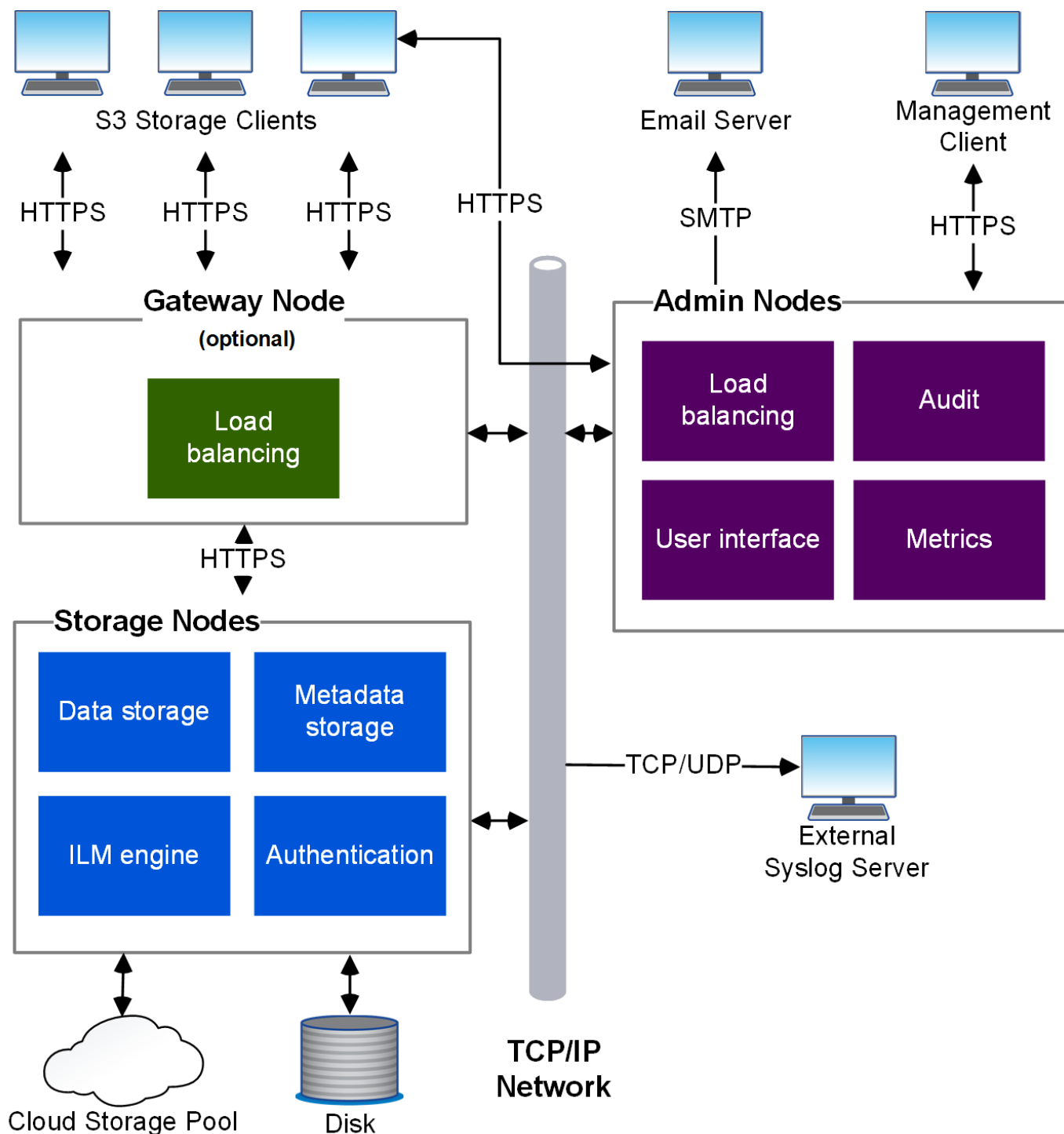
Plusieurs sites logiques peuvent également exister au sein d'un même centre de données pour permettre l'utilisation de la réplication distribuée et du codage d'effacement pour une disponibilité et une résilience accrues.

Redondance des nœuds du grid

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

Architecture du système

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



Les clients S3 stockent et récupèrent des objets dans StorageGRID. D'autres clients sont utilisés pour accéder à l'interface de gestion de StorageGRID et, en option, au partage d'audit. De plus, StorageGRID peut, en option, envoyer des alertes par e-mail via un serveur SMTP externe.

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

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

Grid, nœuds et services

Nœuds et services de la grille StorageGRID

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

Types de nœuds grid

Le système StorageGRID utilise trois types de nœuds de grille :

Nœuds d'administration

Fournissez des services de gestion tels que la configuration système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager, vous vous connectez à un Admin Node. Chaque grid doit avoir un Admin Node principal et peut avoir des Admin Nodes non principaux supplémentaires pour la redondance. Vous pouvez vous connecter à n'importe quel Admin Node, et chaque Admin Node affiche une vue similaire du système StorageGRID. Cependant, vous devez effectuer la plupart des procédures de maintenance à l'aide de l'Admin Node 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

Gestion et stockage des données d'objet et des métadonnées Chaque site de votre système StorageGRID doit avoir au moins trois nœuds de stockage.

Lors de l'installation initiale d'un nouveau nœud de stockage, vous pouvez spécifier qu'il ne soit utilisé que pour "[stocker soit des métadonnées, soit des données](#)".

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

Nœuds de passerelle (en option)

Fournissez une interface d'équilibrage de charge que les applications client peuvent utiliser pour se connecter à StorageGRID. Un équilibreur de charge dirige de manière transparente les clients vers un nœud de stockage optimal, de sorte que la défaillance de nœuds ou même d'un site entier soit transparente.

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. Le nombre maximal de nœuds (y compris tous les types de nœuds) par système est de 220.

Nœuds d'appliance StorageGRID

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

Consultez les sections suivantes pour en savoir plus sur les dispositifs disponibles :

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

Nœuds basés sur logiciel

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. Voir ["Installer StorageGRID sur des nœuds logiciels"](#).

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

Des services StorageGRID

Voici la liste complète des services StorageGRID.

Service	Description	Emplacement
Transitaire de service de compte	Fournit une interface permettant au service Load Balancer d'interroger le service Account Service sur des hôtes distants et fournit des notifications sur les modifications de configuration de point de terminaison Load Balancer au service Load Balancer.	Service Load Balancer sur les nœuds d'administration et les nœuds de passerelle
ADC (contrôleur de domaine administratif)	Gère 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 (Audit Management System)	Surveille et consigne tous les événements et transactions système audités dans un fichier journal texte.	Nœuds d'administration
Démon Avahi	Gère mDNS, qui est utilisé pour la résolution de noms et la découverte de services au sein du réseau local.	Tous les nœuds
Service de cache	S'exécute sur des nœuds d'équilibrage de charge (passerelle) et gère un cache local du contenu des objets.	Nœuds de passerelle
Cassandra	Gère la base de données distribuée pour les métadonnées des objets.	Nœuds de stockage (sauf données uniquement)
Cône Cassandra	Répare automatiquement les métadonnées d'objet.	Nœuds de stockage
Service de bloc	Gestion des données avec code d'effacement et des fragments de parité.	Nœuds de stockage

Service	Description	Emplacement
Nœud de gestion de la configuration (CMN)	Gestion des configurations et des tâches de grid à l'échelle du système. Chaque grille dispose d'un service CMN.	Nœud d'administration principal
DDS (Distributed Data Store)	Interfaces avec la base de données Cassandra pour gérer les métadonnées d'objet.	Nœuds de stockage
DMV (Data Mover)	Déplacement des données vers les terminaux cloud	Nœuds de stockage
IP dynamique (dylip)	Surveille la grille pour détecter les changements d'adresse IP dynamiques et met à jour les configurations locales.	Tous les nœuds
gdu-server	Le gestionnaire de tâches backend pour la maintenance et le provisionnement du grid. Accepte les requêtes provenant de <code>mgmt-api</code> et d'autres scripts utilitaires, les valide et répartit chaque action vers le gestionnaire de tâches GDU approprié, comme le provisionnement, l'expansion, la mise hors service et les mises à niveau.	Nœuds d'administration
Grafana	Utilisé pour la visualisation des metrics dans Grid Manager.	Nœuds d'administration
Haute disponibilité	Gère les adresses IP virtuelles à haute disponibilité sur les nœuds configurés sur la page Groupes à haute disponibilité. Ce service est également connu sous le nom de service <i>keepalived</i> .	Nœuds d'administration et de passerelle
Identité (idnt)	Gère les utilisateurs et les groupes locaux, l'authentification et fédère les identités des utilisateurs à partir de LDAP et d'Active Directory.	Nœuds de stockage qui utilisent le service ADC
Arbitre lambda	Gère les demandes S3 Select SelectObjectContent.	Tous les nœuds
Équilibreur des charges (nginx-gw)	Équilibrage de la charge du trafic S3 des clients vers les nœuds de stockage	Nœuds d'administration et de passerelle
LDR (routeur de distribution locale)	Gestion du stockage et du transfert de contenu au sein de la grille.	Nœuds de stockage

Service	Description	Emplacement
mgmt-api	L'API backend de Grid Manager. Expose des points de terminaison REST authentifiés pour l'administration de la grille (configuration, surveillance et maintenance), gère les validations et les autorisations, et orchestre les opérations de longue durée. Il s'agit de l'API principale du plan de contrôle utilisée par l'interface de Grid Manager et les clients d'automatisation.	Nœuds d'administration
MISCd information Service Control Daemon	Fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, telles que interroger l'état des services exécutés sur d'autres nœuds.	Tous les nœuds
nginx	Agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de grid (Prometheus et IP dynamique, par exemple), afin de pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
Équilibreur de charge nginx-gw	Équilibrage de la charge du trafic S3 des clients vers les nœuds de stockage	Nœuds d'administration et de passerelle
Système de gestion de réseau (NMS)	Alimente les options de surveillance, de rapport et de configuration qui sont affichées via le gestionnaire de grille.	Nœuds d'administration
Exportateur de nœuds (collecte de données Prometheus)	Publie des statistiques au niveau du système pour la collecte de mesures de séries chronologiques Prometheus.	Tous les nœuds
NTP	Service de protocole de temps réseau (NTP).	Tous les nœuds
La persistance des données	Gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage.	Tous les nœuds
Prometheus	Collecte des metrics de séries chronologiques à partir des services sur tous les nœuds.	Nœuds d'administration
RSM (machine d'état répliquée)	S'assure que les demandes de service de la plate-forme sont envoyées à leurs terminaux respectifs.	Nœuds de stockage qui utilisent le service ADC

Service	Description	Emplacement
SSM (moniteur d'état du serveur)	Surveille l'état du matériel et communique des rapports au service NMS.	Une instance est présente sur chaque nœud de grille
Gestionnaire de serveur	Gère les services StorageGRID .	Tous les nœuds
Agent SNMP	Répond aux requêtes SNMP.	Nœuds d'administration
Service de gestion des ports SNMP	Gère la gestion dynamique des ports SNMP.	Tous les nœuds
SSH (Shell sécurisé)	Gère l'accès sécurisé et la gestion du système à distance.	Tous les nœuds
SSM (Moniteur d'état du système)	Surveille l'état du matériel et communique des rapports au service NMS.	Tous les nœuds
Statistique	Enregistre des métriques supplémentaires liées aux buckets S3.	Nœuds de stockage
Agent de traçage (agent Jaeger)	Reçoit et traite les informations de traçage soumises par le collecteur de traces (jaeger-collector).	Tous les nœuds
Collectionneur de traces (jaeger-collector)	Effectue la collecte des traces afin de recueillir des informations à utiliser par le support technique. Le service de collecteur de trace utilise le logiciel Open Source Jaeger.	Nœuds d'administration

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

Des nœuds d'administration qui assurent les 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 grid doit être connecté à un nœud d'administration principal et doit comporter un nombre quelconque de nœuds d'administration non primaires pour assurer la redondance.

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 du nœud d'administration principal.

Le tableau récapitule les fonctionnalités des nœuds d'administration primaires et non primaires.

Capacités	Nœud d'administration principal	Nœud d'administration non primaire
Comprend le AMS service	Oui	Oui
Comprend le CMN service	Oui	Non
Comprend le NMS service	Oui	Oui
Comprend le Prometheus service	Oui	Oui
Comprend le SSM service	Oui	Oui
Inclut les Équilibreur de charge services et Haute disponibilité	Oui	Oui
Prend en charge le Interface du programme d'application de gestion (api de gestion)	Oui	Oui
Peut être utilisé pour toutes les tâches de maintenance réseau, par exemple la modification d'adresse IP et la mise à jour de serveurs NTP	Oui	Non
Peut télécharger le package de récupération	Oui	Oui
Peut effectuer un rééquilibrage du code d'effacement après l'extension du nœud de stockage	Oui	Non
Peut être utilisé pour la procédure de restauration de volume	Oui	Oui
Peut collecter des fichiers journaux et des données système à partir d'un ou plusieurs nœuds	Oui	Oui
Peut récupérer le stockage, la passerelle et les nœuds d'administration non principaux	Oui	Oui
Peut récupérer le nœud d'administration principal	Oui	Oui
Envoie des notifications d'alerte, des packages AutoSupport, des traps et des notifications SNMP	Oui. Agit comme le expéditeur préféré .	Oui. Sert d'émetteur 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, les traps et les notifications 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 expéditeurs de secours.

Plusieurs notifications peuvent être envoyées dans ces cas :

- Si les nœuds d'administration sont « débarqués » les uns des autres, l'expéditeur préféré et les expéditeurs en veille essayeront d'envoyer des notifications et plusieurs copies de notifications peuvent être reçues.
- Si un 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'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité.

Services primaires pour les nœuds d'administration

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

Service	Fonction de touche
système de gestion de l'audit (AMS)	Suit l'activité et les événements du système.
nœud de gestion de la configuration (CMN)	Gestion de la configuration à l'échelle du système.
[[haute disponibilité]]haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. Remarque : ce service se trouve également sur les nœuds de passerelle.
[[équilibreur de charge]]équilibreur de charge	Équilibrage de la charge du trafic S3 des clients vers les nœuds de stockage Remarque : ce service se trouve également sur les nœuds de passerelle.
interface de programme d'application de gestion (mgmt-api)	Traite les requêtes à partir de l'API de gestion Grid et de l'API de gestion des locataires.
système de gestion de réseau (NMS)	Fournit des fonctionnalités pour le gestionnaire de grille.

Service	Fonction de touche
Prometheus	Collecte et stocke les mesures de séries chronologiques des services sur tous les nœuds.
moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Qu'est-ce qu'un nœud de stockage StorageGRID ?

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

Chaque site de votre système StorageGRID doit avoir au moins trois nœuds de stockage.

Types de nœuds de stockage

Pendant l'installation, vous pouvez sélectionner le type de nœud de stockage à installer. Ces types sont disponibles pour les nœuds de stockage logiciels et pour les nœuds de stockage basés sur l'appliance qui prennent en charge cette fonctionnalité :

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

Vous pouvez sélectionner le type de nœud de stockage dans les situations suivantes :

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

Nœud de stockage des données et des métadonnées (combiné)

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

Nœud de stockage des métadonnées uniquement

L'utilisation d'un nœud de stockage exclusivement pour les métadonnées peut être logique si votre grille stocke un très grand nombre de petits objets. L'installation d'une capacité de métadonnées dédiée assure un meilleur équilibre entre l'espace nécessaire pour un très grand nombre d'objets de petite taille et l'espace requis pour les métadonnées de ces objets. Par ailleurs, les nœuds de stockage de métadonnées uniquement hébergés sur des appliances haute performance peuvent améliorer les performances.

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

- Lorsque vous utilisez des appliances StorageGRID, vous ne pouvez configurer que des nœuds uniquement de métadonnées sur les appliances SGF6112 avec douze disques de 1,9 To ou douze disques de 3,8 To.
- Lors de l'utilisation de nœuds logiciels, vous devez vous assurer que les ressources des nœuds uniquement de métadonnées correspondent aux ressources des nœuds de stockage existants. Par exemple :

- Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds exclusivement basés sur des métadonnées logicielles doivent respecter la configuration minimale suivante :
 - 128 GO DE RAM
 - Processeur 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 existants. Les ressources d'un nouveau site doivent correspondre aux nœuds de stockage des sites existants.



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

Nœud de stockage des données uniquement

Il est logique d'utiliser un nœud de stockage exclusivement pour les données si les performances de vos nœuds de stockage diffèrent. Par exemple, pour augmenter les performances, vous pouvez disposer de nœuds de stockage sur disque rotatif haute capacité uniquement en données et accompagnés de nœuds de stockage haute performance pour métadonnées uniquement.

De plus, vous pouvez obtenir davantage de capacité de métadonnées en supprimant les nœuds à faible RAM de Cassandra, ce qui augmente la limite de capacité de métadonnées par nœud. "[Gérer le stockage des métadonnées d'objet](#)".

Vous pouvez convertir un nœud de stockage combiné en un nœud de stockage dédié aux données. Si le nœud de stockage contient le [Service ADC](#) et que les conditions préalables à la conversion sont remplies, le service est automatiquement déplacé vers un autre nœud de stockage du même site pendant la conversion. Pour connaître les conditions préalables et la procédure détaillée, consultez "[Convertir un nœud de stockage en nœud de données uniquement](#)".

Nœuds de stockage requis par grille et par site

Lors de la sélection des nœuds de stockage à utiliser dans votre topologie, gardez à l'esprit que la grille ou chaque site de la grille doit contenir les éléments suivants :

- Par site (dans une grille mono ou multi-sites) : Trois [ADC](#) Nœuds de stockage (peuvent être n'importe quelle combinaison de nœuds de stockage combinés et de métadonnées uniquement)
- Grille à site unique : au moins deux nœuds de stockage d'objets (peut être n'importe quelle combinaison de combinés et de données uniquement)
- Grille multisite : au moins un nœud de stockage d'objets par site (peut être combiné ou réservé aux données)

Services primaires des nœuds de stockage

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



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

Service	Fonction de touche
Compte (compte)	Gestion des comptes de locataire. Les nœuds de stockage de données uniquement n'hébergent pas ce service.
Contrôleur de domaine administratif (ADC)	Maintien de la topologie et de la configuration dans l'ensemble du grid. Les nœuds de stockage de données uniquement n'hébergent pas ce service. Détails Le service contrôleur de domaine d'administration (ADC) authentifie les nœuds de la grille et leurs connexions entre eux. Le service ADC est hébergé sur au moins trois nœuds de stockage sur un site. Le service ADC gère les informations de topologie, notamment la localisation et la disponibilité des services. Lorsqu'un nœud du grid a besoin d'informations provenant d'un autre nœud du grid ou d'une action à effectuer par un autre nœud du grid, il contacte un service ADC pour trouver le meilleur nœud du grid afin de traiter sa requête. De plus, le service ADC conserve une copie des bundles de configuration du déploiement StorageGRID, permettant à tout nœud du grid de récupérer les informations de configuration actuelles. Pour faciliter les opérations distribuées et en attente, chaque service ADC synchronise les certificats, les lots de configuration et les informations sur les services et la topologie avec les autres services ADC du système StorageGRID. En général, tous les nœuds de la grille maintiennent une connexion à au moins un service ADC. Les nœuds du grid accèdent ainsi aux informations les plus récentes. Lorsque les nœuds de grille se connectent, ils mettent en cache les certificats des autres nœuds de grille, ce qui permet aux systèmes de continuer à fonctionner avec des nœuds de grille connus même lorsqu'un service ADC est indisponible. Les nouveaux nœuds de grille ne peuvent établir de connexions qu'à l'aide d'un service ADC. La connexion de chaque nœud de grille permet au service ADC de collecter les informations de topologie. Ces informations sur le nœud de la grille incluent la charge CPU, l'espace disque disponible (si le système dispose de stockage), les services pris en charge et l'ID de site du nœud de la grille. D'autres services demandent au service ADC d'obtenir des informations sur la topologie par le biais de requêtes de topologie. Le service ADC répond à chaque requête avec les dernières informations reçues du système StorageGRID.

Service	Fonction de touche
Cassandra	Stocke et protège les métadonnées d'objet. Les nœuds de stockage de données uniquement n'hébergent pas ce service.
Cône Cassandra	Répare automatiquement les métadonnées d'objet. Les nœuds de stockage de données uniquement n'hébergent pas ce service.
Bloc	Gestion des données avec code d'effacement et des fragments de parité.
Data Mover (dmv)	Déplacement des données vers des pools de stockage cloud.
Stockage de données distribué (DDS)	Surveille le stockage des métadonnées d'objet. Détails Chaque nœud de stockage inclut le service DDS (Distributed Data Store). Ce service assure l'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 par le système (S3).
Identité (idnt)	Fédération des identités d'utilisateur à partir de LDAP et d'Active Directory. Les nœuds de stockage de données uniquement n'hébergent pas ce service.

Service	Fonction de touche
routeur de distribution locale (LDR)	Traite les demandes de protocole de stockage objet et gère les données d'objet sur le disque.

Service	Fonction de touche
RSM (Replicated State machine)	Envoi des demandes de services de la plateforme S3 à leurs terminaux respectifs Les nœuds de stockage de données uniquement n'hébergent pas ce service.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

données et les fonctions de trafic de données.

Qu'est-ce qu'un nœud de passerelle StorageGRID ?

Le service LDR gère les tâches suivantes :

Les nœuds de passerelle fournissent une interface dédiée d'équilibrage de la charge que les applications client S3 peuvent utiliser pour se connecter à StorageGRID. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage. Les nœuds de passerelle sont facultatifs.

- Requetes
- Activité liée à la gestion du cycle de vie des informations (ILM)
- Suppression d'objet
- Stockage des données objet

Le service StorageGRID Load Balancer est fourni sur tous les nœuds d'administration et sur tous les nœuds de passerelle. Il effectue la résiliation du protocole TLS (transport Layer Security) des requêtes du client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage. Le service Load Balancer dirige les clients de **Gestion du stockage des données** vers le nœud de stockage optimal, de sorte que la défaillance des nœuds, voire d'un site entier, soit transparente.

- Transferts de données objet à partir d'un autre service LDR (nœud de stockage)
- Gestion du stockage des données
- Interface de protocole S3

Vous configurez un ou plusieurs nœuds finaux d'équilibrage de charge pour définir le port et le protocole réseau (HTTPS ou HTTP) que les demandes des clients entrants et sortants utiliseront pour accéder aux services d'équilibrage de charge sur les nœuds d'administration et de passerelle. Le terminal de l'équilibreur de charge définit également le type de client (S3), le mode de liaison et, éventuellement, la liste des locataires autorisés ou bloqués. Voir **"Considérations relatives à l'équilibrage de charge"**.

Magasins d'objets

Le stockage sous-jacent d'un service LDR est divisé en un nombre fixe de magasins d'objets (aussi appelés volumes de stockage). Chaque magasin d'objets est un point de montage distinct.

Si nécessaire, vous pouvez regrouper les interfaces réseau de plusieurs nœuds de passerelle et nœuds d'administration dans un groupe haute disponibilité. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail de l'application client. Voir **"Gestion des groupes haute disponibilité"**.

Les magasins d'objets d'un nœud de stockage sont identifiés par un nombre hexadécimal compris entre 0000 et 002F, appelé ID de volume.

Services primaires pour les nœuds de passerelle

L'espace est réservé dans le premier magasin d'objets (volume 0) pour les métadonnées d'objet dans une base de données Cassandra. Tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres magasins d'objets sont exclusivement utilisés pour les données d'objet, notamment les copies répliquées et les fragments avec code d'effacement.

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

Service	Fonction de touche
Service de cache	Gère un cache local du contenu de l'objet.
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. Remarque : ce service se trouve également sur les nœuds d'administration.

données Cassandra, qui assure l'interface avec le service LDR.

Pour assurer la redondance et ainsi la protection contre la perte, trois copies des métadonnées d'objet sont conservées sur chaque site. Cette réplification n'est pas configurable et se fait automatiquement. Pour plus de détails, voir **"Gérer le stockage des métadonnées d'objet"**.

Service	Fonction de touche
Équilibreur de charge	Équilibrage de la 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 se trouve également sur les noeuds d'administration.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

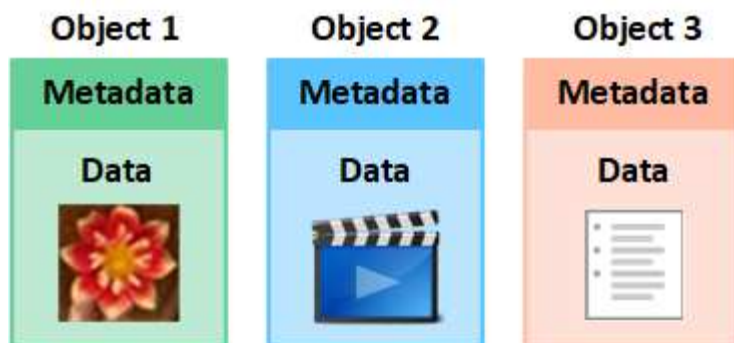
La gestion des données par StorageGRID

Qu'est-ce qu'un objet StorageGRID

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

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

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



Qu'est-ce que les données d'objet ?

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

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

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

Les métadonnées de l'objet incluent les informations suivantes :

- Métadonnées du 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 création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.

- Emplacement de stockage actuel de chaque copie d'objet ou fragment codé d'effacement.
- Toutes les métadonnées utilisateur associées à l'objet.

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

Pour plus d'informations sur la manière et l'emplacement du stockage des métadonnées d'objet par StorageGRID, consultez ["Gérer le stockage des métadonnées d'objet"](#).

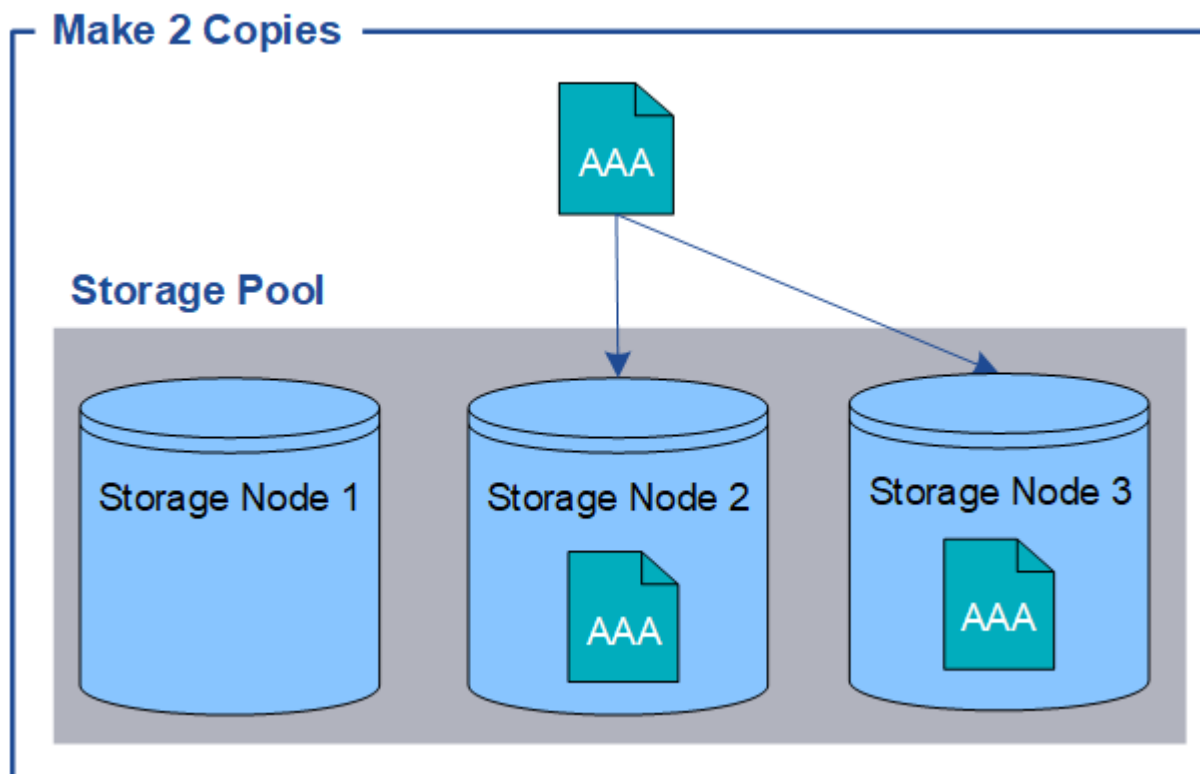
Comment les données d'objet sont-elles protégées ?

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

La réplication

Lorsque StorageGRID 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 en mode objet et les stocke sur des nœuds de stockage ou des pools de stockage cloud. Les règles ILM déterminent le nombre de copies effectuées, l'emplacement de stockage de ces copies et la durée pendant laquelle elles sont conservées par le système. Par exemple, en cas de perte d'une copie suite à la perte d'un nœud de stockage, l'objet est toujours disponible si une copie de celui-ci existe ailleurs dans le système StorageGRID.

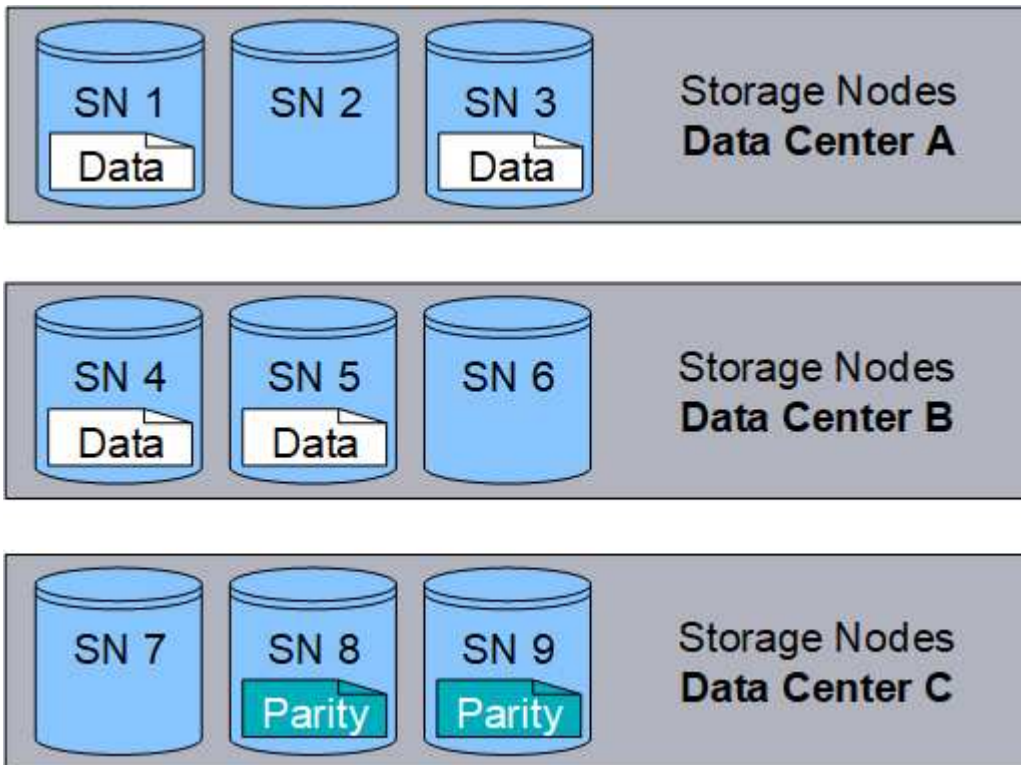
Dans l'exemple suivant, la règle Make 2 copies spécifie que deux copies répliquées de chaque objet sont placées dans un pool de stockage contenant trois nœuds de stockage.



Le code d'effacement

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

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



Informations associées

- ["Gestion des objets avec ILM"](#)
- ["Utilisation de la gestion du cycle de vie des informations"](#)

Cycle de vie des objets dans StorageGRID

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

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

- **Ingest** : processus d'une application client S3 enregistrant 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 avec code d'effacement dans StorageGRID, tel que décrit par les règles ILM des règles ILM actives. Pendant la 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.
- **Retrieve** : processus d'accès d'une application client 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** : processus de suppression de toutes les copies d'objet de la grille. Ces objets peuvent être supprimés suite à l'envoi d'une requête de suppression au système StorageGRID ou à un processus automatique exécuté par StorageGRID au moment où sa durée de vie arrive à expiration.



Informations associées

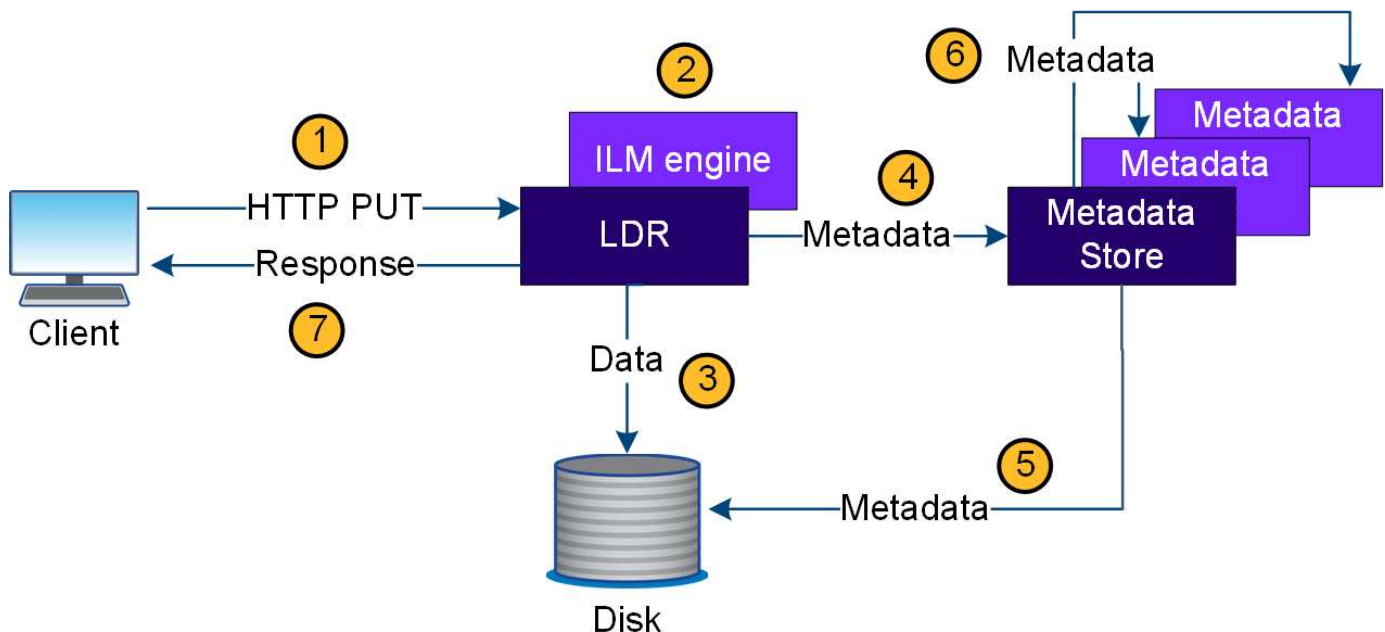
- ["Gestion des objets avec ILM"](#)
- ["Utilisation de la gestion du cycle de vie des informations"](#)

Comment StorageGRID gère l'ingestion d'objets

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

Flux de données

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



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

Comment StorageGRID gère les copies d'objets

Les données d'objet sont gérées par les politiques ILM actives et les règles ILM associées. Les règles ILM permettent de réaliser des copies répliquées ou avec code d'effacement pour protéger les données en mode objet contre la perte.

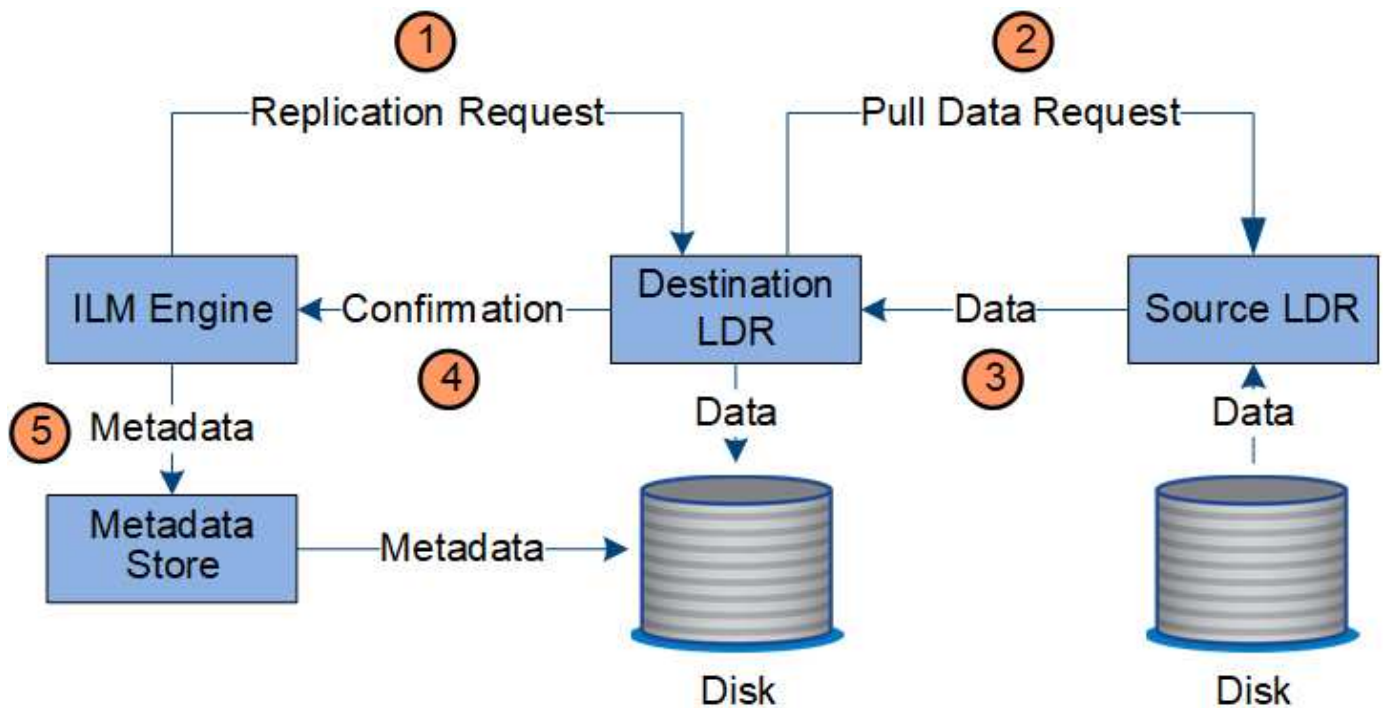
Différents types ou emplacements de copies d'objets peuvent être requis à différents moments de la vie de l'objet. Les règles ILM sont régulièrement évaluées afin de s'assurer que les objets sont placés en fonction des besoins.

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

Protection du contenu : réplication

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

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

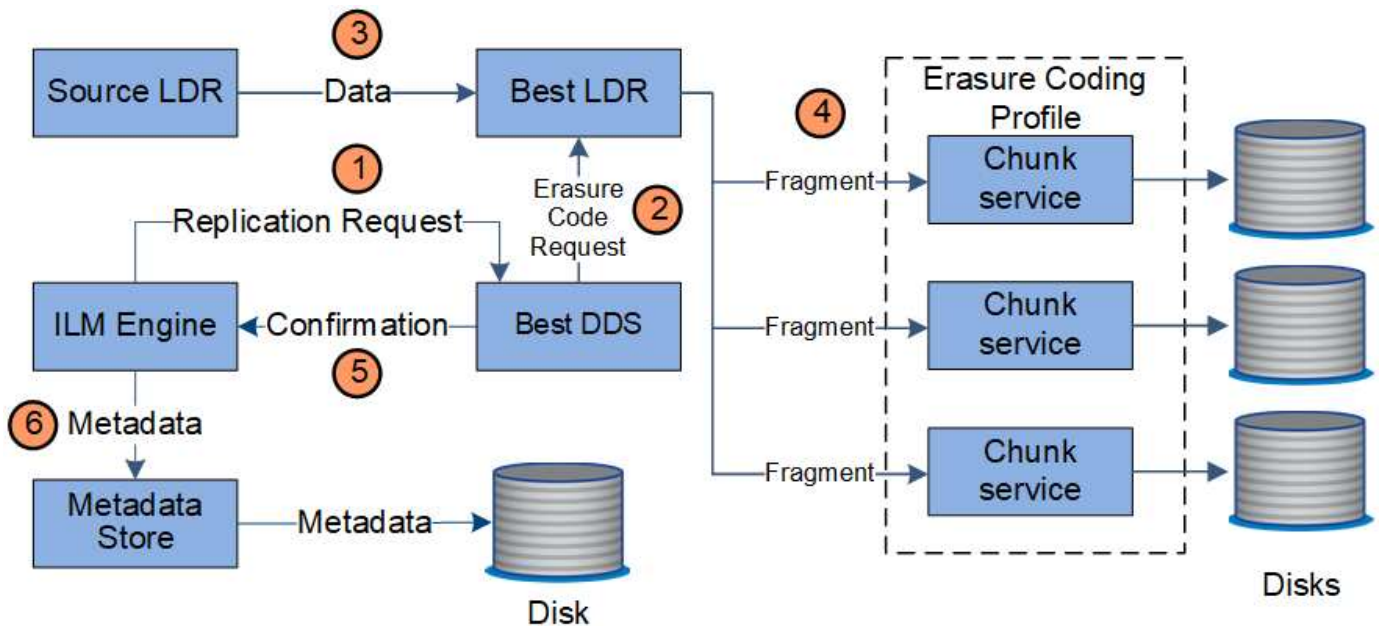


1. Le moteur ILM interroge le service ADC afin de déterminer le meilleur service LDR de destination au sein du pool de stockage spécifié par la règle ILM. Il envoie ensuite une commande au service LDR pour lancer la réplication.
2. Le service LDR de destination interroge le service ADC pour obtenir le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

Protection du contenu : code d'effacement

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

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

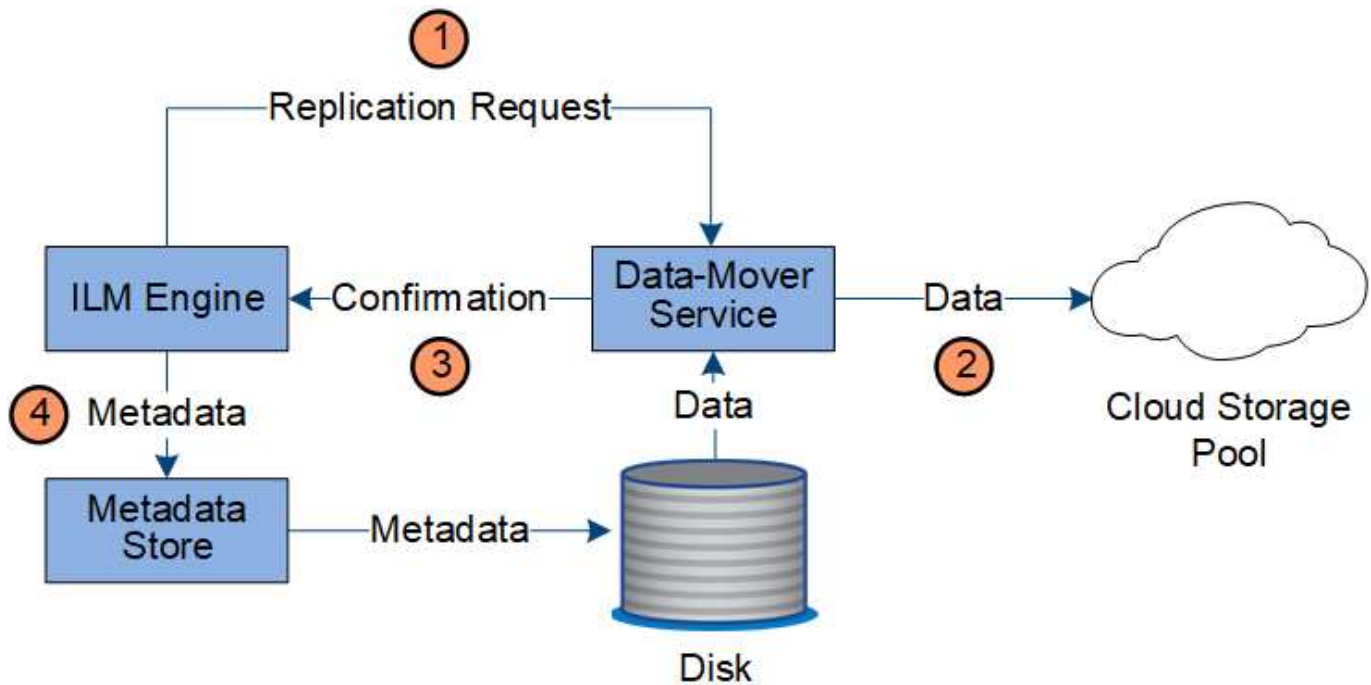


1. Le moteur ILM interroge le service ADC afin de déterminer quel service DDS peut le mieux effectuer l'opération de codage d'effacement. Lorsqu'il est déterminé, le moteur ILM envoie une demande d'initialisation à ce service.
2. Le service DDS demande à un LDR de coder les données de l'objet.
3. Le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

Protection du contenu : pool de stockage cloud

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

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



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

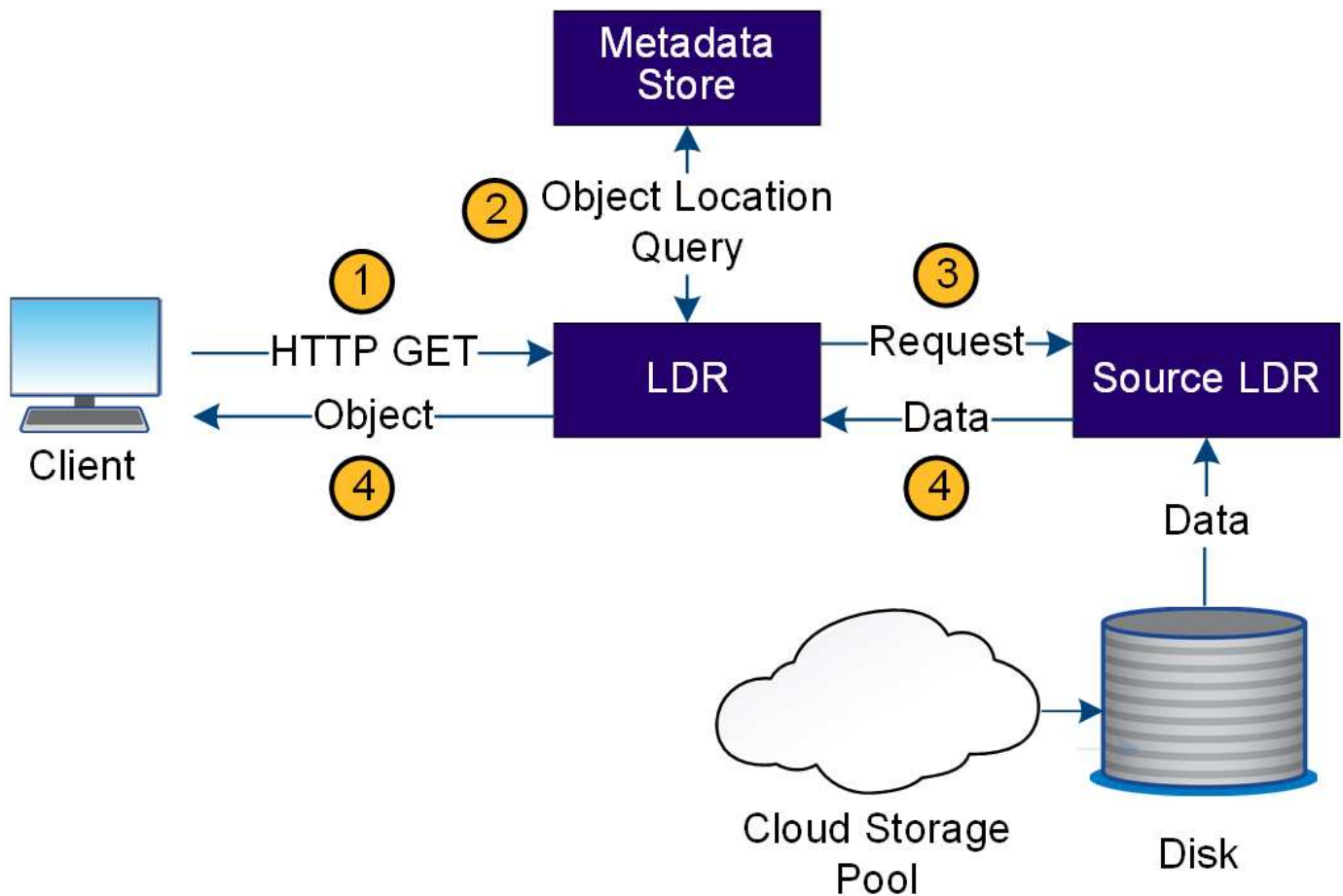
Comment StorageGRID gère la récupération des objets

Une opération de récupération se compose d'un flux de données défini entre le système StorageGRID et le client. Le système utilise des attributs pour suivre l'extraction 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 afin d'obtenir l'emplacement des données d'objet et les récupère à partir du service LDR source. De préférence, la récupération se fait à partir d'un nœud de stockage. Si l'objet n'est pas disponible sur un nœud de stockage, la demande de récupération est dirigée vers un pool de stockage cloud.



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



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

Comment StorageGRID gère la suppression d'objets

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

Hiérarchie de suppression

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

- **Verrouillage d'objet S3** : si le paramètre de verrouillage d'objet S3 global est activé pour la grille, les clients S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation à jour et de conservation légale pour chaque version

d'objet ajoutée à ce compartiment.

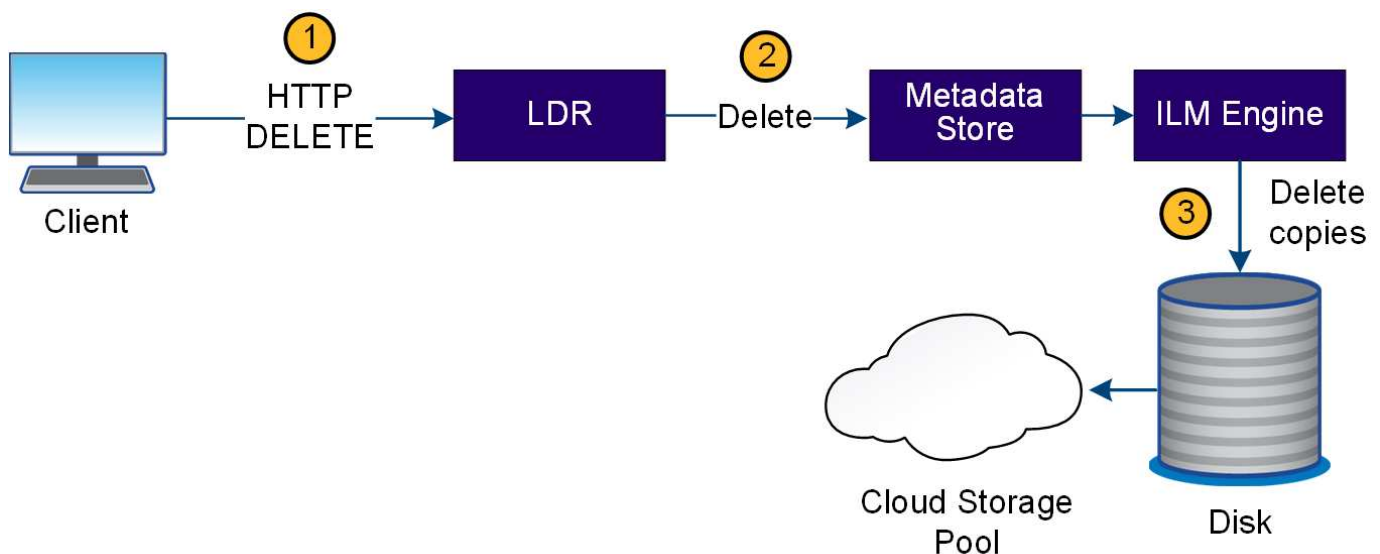
- Aucune méthode ne permet de supprimer une version d'objet faisant l'objet d'une conservation légale.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut pas être supprimée par aucune méthode.
 - Les objets d'un compartiment lorsque le verrouillage d'objet S3 est activé sont conservés « indéfiniment » par la règle ILM. Une fois la date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou l'expiration du cycle de vie du compartiment.
 - Si les clients S3 appliquent une date de conservation jusqu'au compartiment par défaut, ils n'ont pas besoin de spécifier une date de conservation jusqu'à pour chaque objet.
- **Requête de suppression client** : un client S3 peut émettre une requête de suppression d'objet. Lorsqu'un client supprime un objet, toutes les copies de cet objet sont supprimées du système StorageGRID.
 - **Supprimer les objets dans le compartiment** : les utilisateurs du gestionnaire de locataires peuvent utiliser cette option pour supprimer définitivement toutes les copies des objets et des versions d'objet dans les compartiments sélectionnés du système StorageGRID.
 - **Cycle de vie des compartiments S3** : les clients S3 peuvent ajouter une configuration de cycle de vie à leurs compartiments qui spécifie une action d'expiration. Lorsqu'il existe un cycle de vie de compartiment, StorageGRID supprime automatiquement toutes les copies d'un objet lorsque la date ou le nombre de jours spécifiés dans l'action d'expiration sont atteints, à moins que le client n'ait supprimé l'objet en premier.
 - **Instructions de placement ILM** : en supposant que le verrouillage objet S3 n'est pas activé dans le compartiment et qu'il n'y a pas de cycle de vie de compartiment, StorageGRID supprime automatiquement un objet lorsque la dernière période de la règle ILM se termine et qu'aucun autre placement n'est spécifié pour l'objet.



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

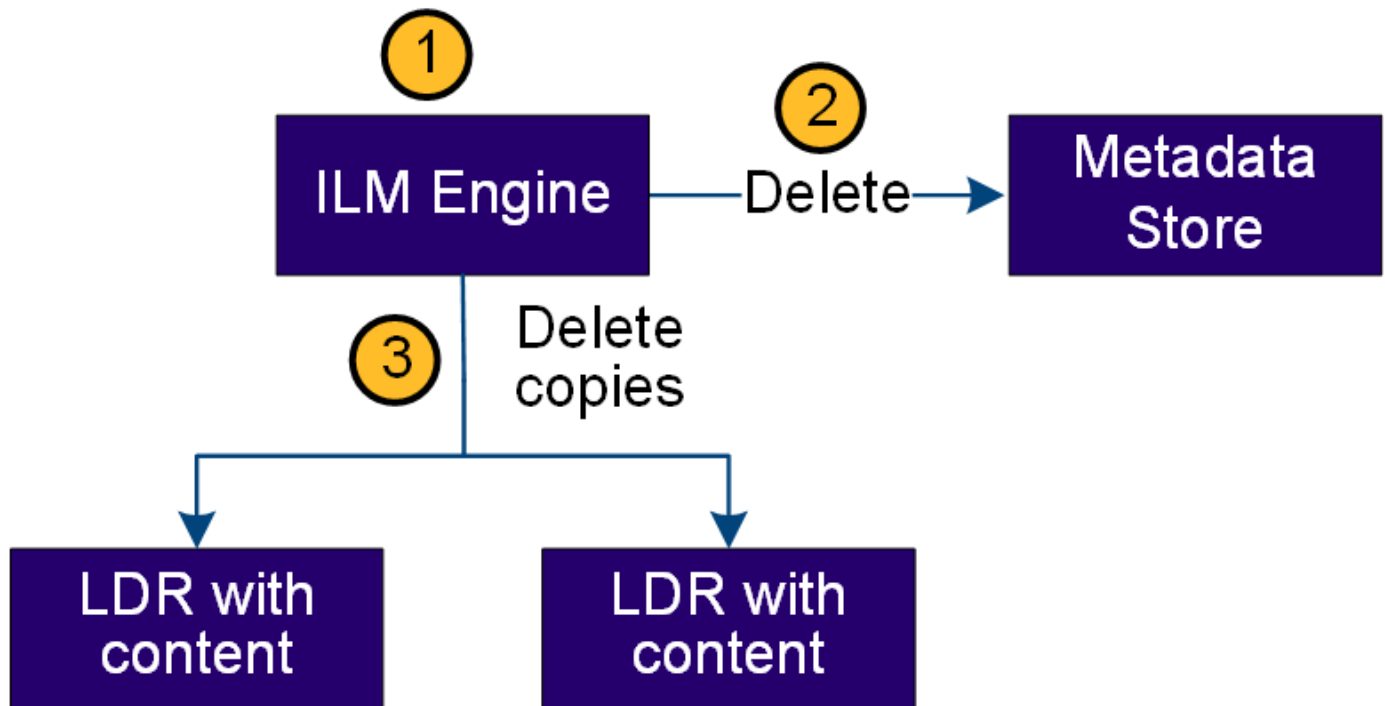
Voir "[Comment supprimer les objets](#)" pour plus d'informations.

Flux de données pour les suppressions client



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

Flux de données pour les suppressions ILM



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

Gestion du cycle de vie des informations dans StorageGRID

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 peut avoir plusieurs politiques actives à la fois.

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 compartiments S3 spécifiques ou à des valeurs de métadonnées spécifiques.
- Type et emplacement de stockage. Les objets peuvent être stockés sur des nœuds de stockage ou dans

des pools de stockage cloud.

- Le type de copie d'objet effectuée. Les copies peuvent être répliquées ou avec code d'effacement.
- Pour les copies répliquées, le nombre de copies effectuées.
- Pour les copies avec code d'effacement, le schéma de code d'effacement utilisé.
- Évolution au fil du temps vers l'emplacement de stockage et le type de copies d'un objet
- La protection des données objet lors de l'ingestion des objets dans la grille (placement synchrone ou double allocation).

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

Exemple de règle ILM

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

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

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

Évaluation des objets par une règle ILM

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

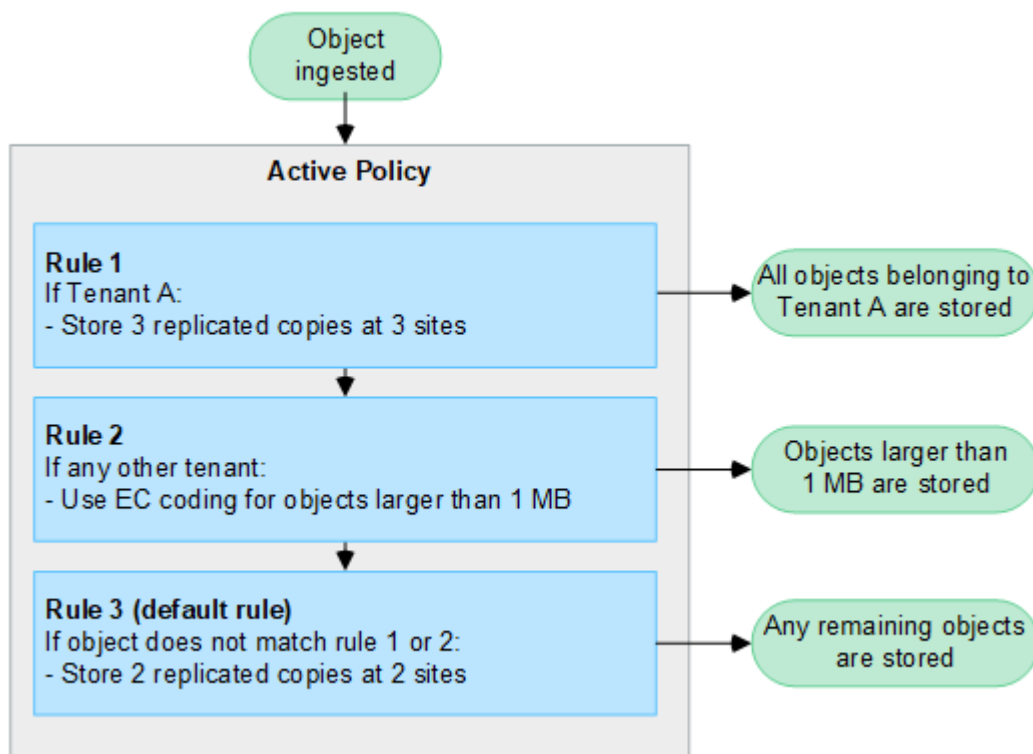
Lorsque des clients enregistrent des objets dans StorageGRID, les objets sont évalués en fonction du jeu ordonné de règles ILM de la politique active, comme suit :

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

Exemple de règle ILM

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

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



Informations associées

- ["Gestion des objets avec ILM"](#)

Découvrez StorageGRID

Explorez le gestionnaire de grille StorageGRID

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



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

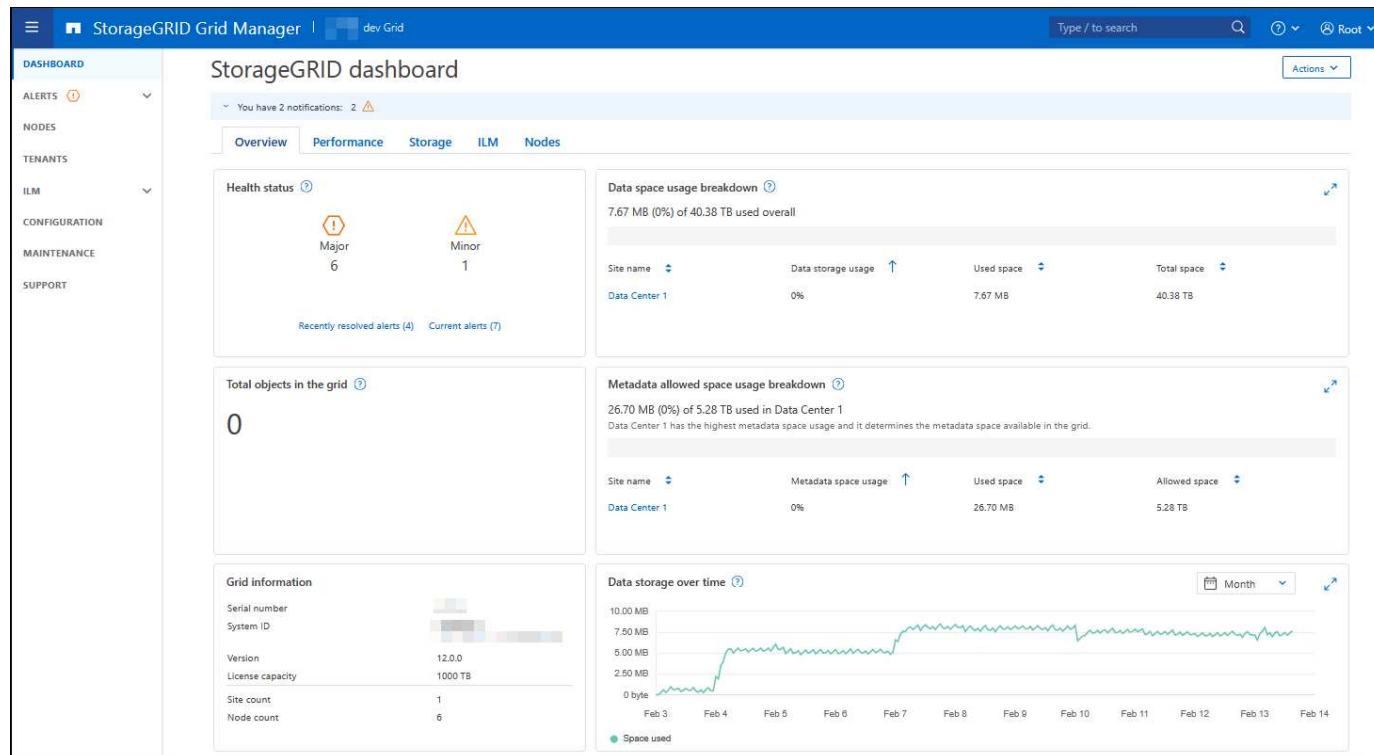
Lorsque vous vous connectez à Grid Manager, vous vous connectez à un nœud d'administration. Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non primaires. Vous pouvez vous connecter à n'importe quel nœud d'administration et chaque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

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

Tableau de bord de Grid Manager

Lorsque vous vous connectez pour la première fois au Gestionnaire de grille, vous pouvez utiliser le tableau de bord pour ["surveiller les activités du système"](#) obtenir un aperçu.

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. Vous pouvez ["configurer le tableau de bord"](#) choisir parmi une collection de cartes contenant les informations dont vous avez besoin pour surveiller efficacement votre système.



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

Champ de recherche

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

Vous pouvez utiliser **Search** pour rechercher des entrées dans la barre latérale du Gestionnaire de grille et dans les menus Configuration, Maintenance et support. Vous pouvez également rechercher par nom des

éléments tels que les nœuds de grid et les comptes de locataire.

Menu aide

Le menu d'aide  donne accès à :

- Le ["FabricPool"](#) et ["Configuration de S3"](#) sorciers
- Le site de documentation StorageGRID pour la version actuelle
- ["Documentation de l'API"](#)
- Informations sur la version de StorageGRID actuellement installée

Menu alertes

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

Dans le menu alertes, vous pouvez effectuer les opérations suivantes ["gestion des alertes"](#):

- Examiner les alertes en cours
- Examiner les alertes résolues
- Configurez les silences pour supprimer les notifications d'alerte
- Définissez des règles d'alerte pour les conditions qui déclenchent des alertes
- Configurer les notifications par e-mail pour les alertes StorageGRID

Page nœuds

Le ["Page nœuds"](#) affiche des informations sur l'ensemble de la grille, chaque site de la grille et chaque nœud d'un site. Pour afficher les informations d'un site ou d'un nœud particulier, sélectionnez le site ou le nœud.

Page locataires

Le ["Page locataires"](#) vous permet de ["créer et contrôlez les comptes de locataires du stockage"](#) le faire pour votre système StorageGRID. Vous devez créer au moins un compte de tenant pour spécifier qui peut stocker et récupérer des objets et la fonctionnalité qui leur est disponible.

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

Menu ILM

Le système ["Menu ILM"](#) vous permet ["Configuration des règles et des règles de gestion du cycle de vie des informations \(ILM\)"](#) de gérer la durabilité et la disponibilité des données. Vous pouvez également saisir un identifiant d'objet pour afficher les métadonnées de cet objet.

Le menu ILM permet de consulter et de gérer les informations ILM :

- Règles
- Stratégies
- Balises de stratégie
- Pools de stockage

- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet

Menu Configuration

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

Tâches réseau

Les tâches réseau incluent :

- ["Gérez les groupes haute disponibilité"](#)
- ["Gérer les points de terminaison de l'équilibreur de charge"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)
- ["Gérer les stratégies de classification du trafic"](#)
- ["Configurez les interfaces VLAN"](#)
- ["Activer StorageGRID CORS pour une interface de gestion"](#)

Tâches de sécurité

Les tâches de sécurité comprennent :

- ["Gérer les certificats de sécurité"](#)
- ["Gérer les contrôles de pare-feu internes"](#)
- ["Configurer les serveurs de gestion des clés"](#)
- Configurer les paramètres de sécurité, y compris le ["Règles TLS et SSH"](#), ["options de sécurité du réseau et des objets"](#), ["paramètres de sécurité de l'interface"](#), et ["Options d'accès SSH"](#)
- Configurer les paramètres pour un ["proxy de stockage"](#) ou un ["proxy d'administration"](#)

Tâches système

Les tâches système incluent :

- Utilisez ["fédération des grilles"](#) pour synchroniser les informations des comptes locataires et répliquer les données d'objets entre deux systèmes StorageGRID
- En option, activez le ["Compresser les objets stockés"](#) option
- En option, configurez le ["paramètre de cohérence de compartiment par défaut"](#)
- ["Gérer le verrouillage des objets S3"](#)
- Comprendre les paramètres de stockage tels que ["filigranes de volume de stockage"](#)
- ["Gestion des profils de code d'effacement"](#)

Tâches de surveillance

Les tâches de surveillance incluent :

- "Configurer le serveur de messagerie"
- "Configurer la gestion des journaux"
- "Utiliser la surveillance SNMP"

Tâches de contrôle d'accès

Les tâches de contrôle d'accès comprennent :

- "Gérez les groupes d'administration"
- "Gérer les utilisateurs administrateurs"
- Changer le "phrase secrète de provisionnement" ou "mots de passe de la console de nœuds"
- "Utiliser la fédération des identités"
- "Configurer SSO"
- "Configurer la vérification multi-administrateur"

Menu Maintenance

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

Tâches

Les tâches de maintenance sont les suivantes :

- "Désaffectation des opérations" pour supprimer les sites et les nœuds de grille inutilisés
- "Opérations d'extension" pour ajouter de nouveaux nœuds et sites de grille
- "Procédures de restauration des nœuds de la grille" pour remplacer un nœud défaillant et restaurer les données
- "Renommer les procédures" pour modifier les noms d'affichage de votre grille, de vos sites et de vos nœuds
- "Opérations de vérification de l'existence des objets" pour vérifier l'existence (bien que ce ne soit pas l'exactitude) des données d'objet
- Effectuer une "redémarrage en continu" pour redémarrer plusieurs nœuds de grille
- Restauration des données d'objet
 - "Restaurez les données d'objet vers un volume de stockage pour l'appliance"
 - "Restaurez les données d'objet vers le volume de stockage sur lequel le disque système est intact"
 - "Restauration des données d'objet sur le volume de stockage (panne de disque système)"

Système

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

- "Afficher les informations de licence StorageGRID" ou "mettre à jour les informations de licence"
- Génération et téléchargement du "plan de relance"
- Effectuer des mises à jour logicielles StorageGRID, y compris des mises à niveau logicielles, des correctifs et des mises à jour du logiciel SANtricity OS sur des appliances sélectionnées

- "Procédure de mise à jour"
- "Procédure de correctif"
- "Mise à niveau du système d'exploitation SANtricity sur les contrôleurs de stockage SG6000 à l'aide du gestionnaire de grid"
- "Mise à niveau du système d'exploitation SANtricity sur les contrôleurs de stockage SG5700 à l'aide du gestionnaire de grid"

Le réseau

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

- "Configuration des serveurs DNS"
- "Mettre à jour les sous-réseaux du réseau Grid"
- "Gérer les serveurs NTP"

Menu support

Le menu support fournit des options qui vous aident à analyser et à dépanner votre système.

Outils

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

- "Configurez AutoSupport"
- "Exécuter les diagnostics" sur l'état actuel de la grille
- "Collecte de fichiers journaux et de données système"
- "Examinez les metrics de support"



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

Autre

Dans la section autre du menu support, vous pouvez :

- Configurer "Priorisation des E/S"
- Gérer "coût du lien"
- Afficher les identifiants de service des nœuds
- Gérer "filigranes de stockage"

Explorez le StorageGRID Tenant Manager

Le "[Gestionnaire de locataires](#)" est une interface graphique accessible via un navigateur qui permet aux utilisateurs locataires d'accéder à pour configurer, gérer et contrôler leurs comptes de stockage.



Le Gestionnaire de locataires est mis à jour avec chaque version et peut ne pas correspondre aux captures d'écran d'exemple de cette page.

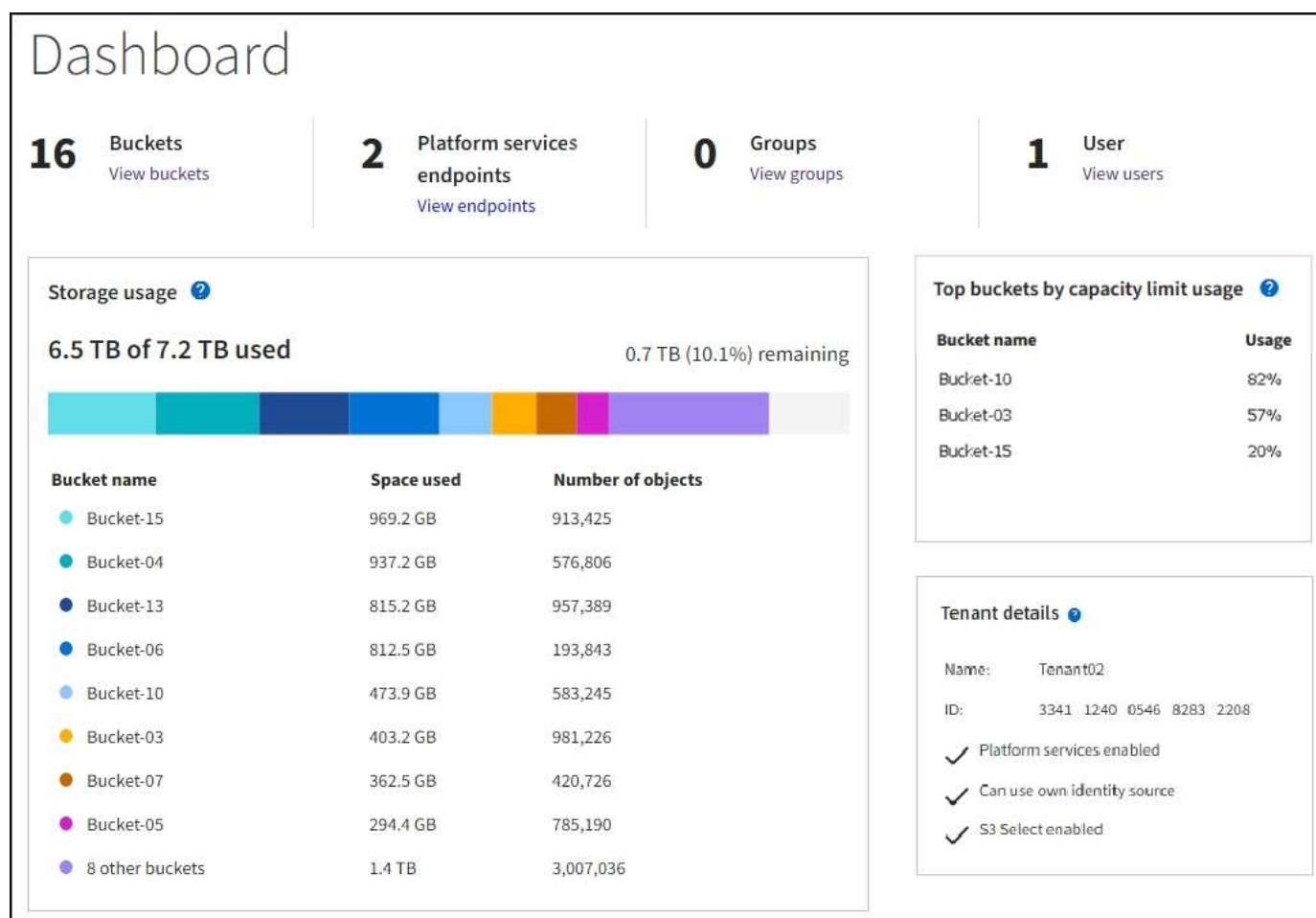
Lorsque les utilisateurs locataires se connectent au Gestionnaire de locataires, ils se connectent à un noeud d'administration.

Tableau de bord du gestionnaire des locataires

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

Le tableau de bord du gestionnaire de locataires permet aux utilisateurs locataires de surveiller l'utilisation du stockage en un coup d'œil. Le panneau d'utilisation du stockage contient une liste des plus grands compartiments S3 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 une somme de l'espace utilisé pour tous les compartiments ou conteneurs du locataire. Si le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets disponibles pour le locataire a été spécifié lors de la création du compte, le volume de quota utilisé et restant est également affiché.



Menu stockage (S3)

Ce menu permet aux utilisateurs de S3 de :

- Gérer les clés d'accès
- Créer, gérer et supprimer des buckets
- Gérez les terminaux des services de plateforme
- Afficher toutes les connexions de fédération de grille qu'ils sont autorisés à utiliser

Mes clés d'accès

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

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



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

Seaux

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

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

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

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

Terminaux des services de plateforme

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

Connexions de fédération de grille

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

Accès au menu gestion

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

Instructions de mise en réseau

Directives de mise en réseau pour StorageGRID

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

À propos de ces instructions

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

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

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

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

Avant de commencer

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

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

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

Installez les nœuds d'appliance

- ["Installez le matériel de l'appliance"](#)

Installation des nœuds basés sur logiciel

- ["Installer StorageGRID sur des nœuds logiciels"](#)

Configuration et administration du logiciel StorageGRID

- ["Administrer StorageGRID"](#)
- ["Notes de mise à jour"](#). Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

Types de réseau StorageGRID

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

Types de trafic

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

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

- Réseau Grid uniquement

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

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

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

Interfaces réseau

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

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

Pour plus de détails sur le mappage des ports virtuels ou physiques aux interfaces réseau des nœuds, voir ["Installer StorageGRID sur des nœuds logiciels"](#) .

Nœuds d'appliance

- ["Système de stockage SG6160"](#)
- ["Système de stockage SGF6112"](#)
- ["Système de stockage SG6000"](#)
- ["Système de stockage SG5800"](#)
- ["Système de stockage SG5700"](#)
- ["Appliances de services SG110 et SG1100"](#)
- ["Appliances de services SG100 et SG1000"](#)

Informations réseau pour chaque nœud

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

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

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

devez utiliser l'adresse IP comme adresse de passerelle.

Groupes haute disponibilité

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

Réseau Grid

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



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

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



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

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

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

Réseau d'administration

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

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

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

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

Le réseau Admin n'est jamais utilisé pour le trafic interne du grid. Une passerelle réseau Admin est fournie et

permet au réseau Admin de communiquer avec plusieurs sous-réseaux externes. Cependant, la passerelle réseau Admin n'est jamais utilisée comme passerelle par défaut du nœud.

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

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

Réseau client

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

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

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

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

- Nœuds de passerelle, car ces nœuds fournissent un accès au service StorageGRID Load Balancer et au client S3 pour la grille.
- Nœuds de stockage, car ces nœuds fournissent l'accès au protocole S3, aux pools de stockage cloud et au service de réplication CloudMirror.
- Nœuds d'administration : pour s'assurer que les utilisateurs locataires peuvent se connecter au gestionnaire des locataires sans avoir à utiliser le réseau d'administration.

Notez les éléments suivants pour la passerelle réseau client :

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

Réseaux VLAN facultatifs

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

Pour prendre en charge l'utilisation des VLAN, vous devez configurer une ou plusieurs interfaces sur un nœud

en tant qu'interfaces de jonction au niveau du commutateur. Vous pouvez configurer l'interface réseau Grid (eth0) ou l'interface réseau client (eth2) en tant que ligne réseau, ou vous pouvez ajouter des interfaces de ligne réseau au nœud.

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

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



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

Reportez-vous à la section "[Configurez les interfaces VLAN](#)" pour obtenir des instructions et des instructions.

Les interfaces VLAN sont utilisées uniquement dans les groupes haute disponibilité et des adresses VIP sont attribuées sur le nœud actif. Reportez-vous à la section "[Gérez les groupes haute disponibilité](#)" pour obtenir des instructions et des instructions.

Exemples de topologie réseau

Topologie du réseau Grid pour StorageGRID

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

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

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

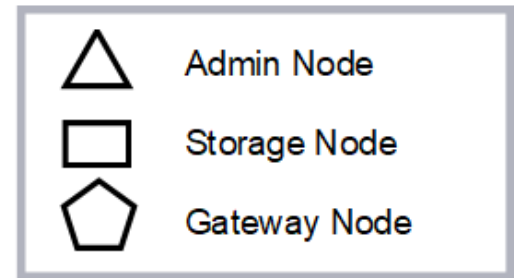
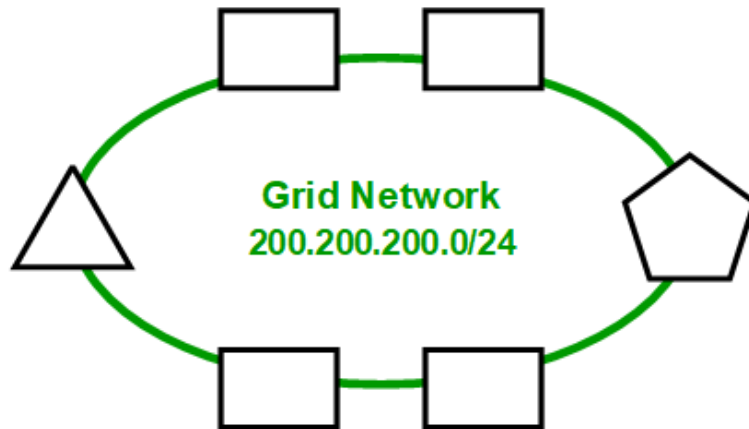
Lors de l'installation, l'interface réseau de grille applique des routes statiques pour tous les sous-réseaux du GNSL et définit la route par défaut du nœud vers la passerelle réseau de grille si elle est configurée. Le GNSL n'est pas nécessaire s'il n'y a pas de réseau client et que la passerelle réseau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

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



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

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 pour StorageGRID

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

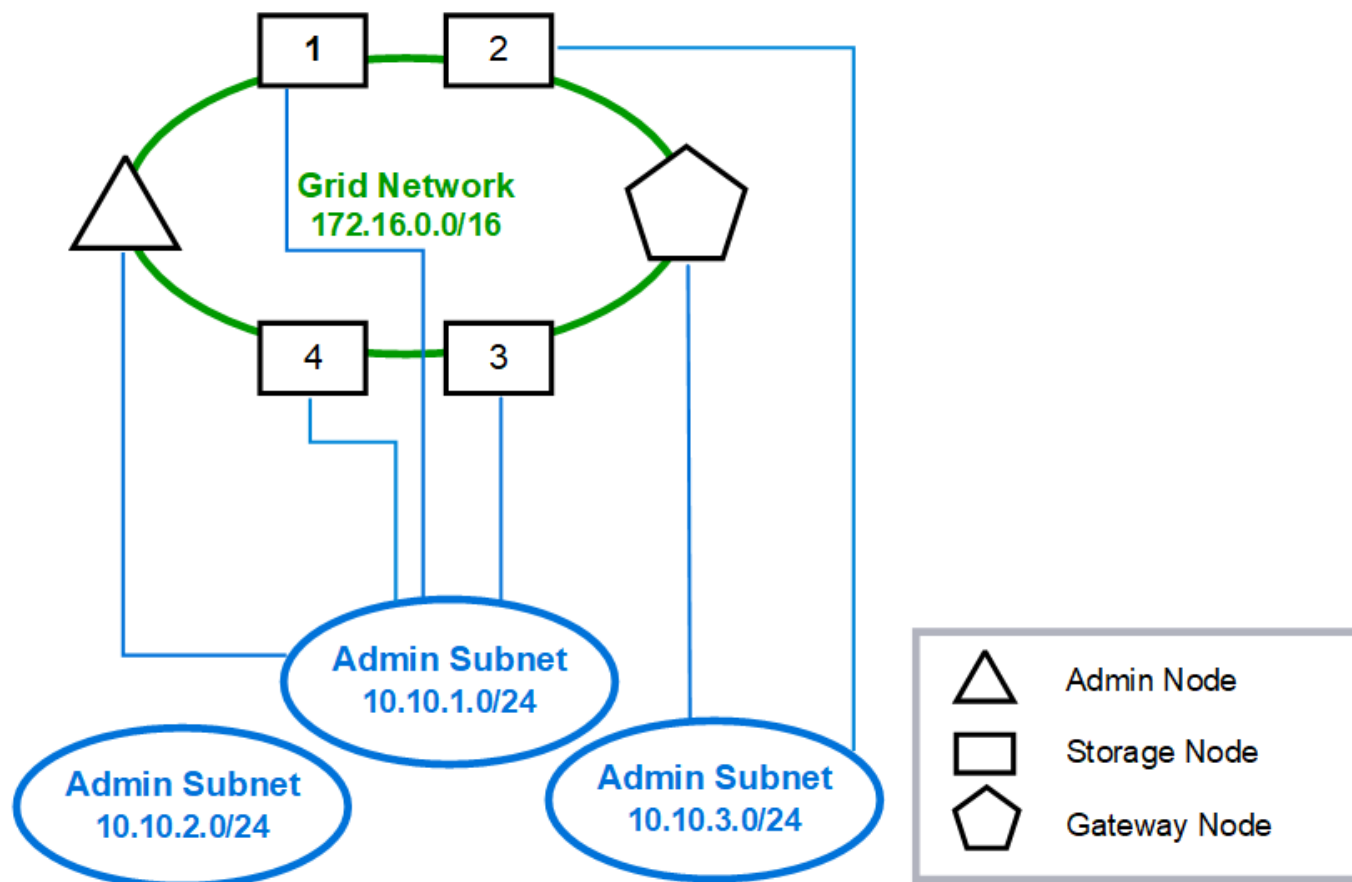
Lorsque vous configurez le réseau Admin, vous définissez l'adresse IP de l'hôte, le masque de sous-réseau et l'adresse IP de la passerelle pour l'interface eth1 de chaque nœud de la grille.

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

l'AESL.

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

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 pour StorageGRID

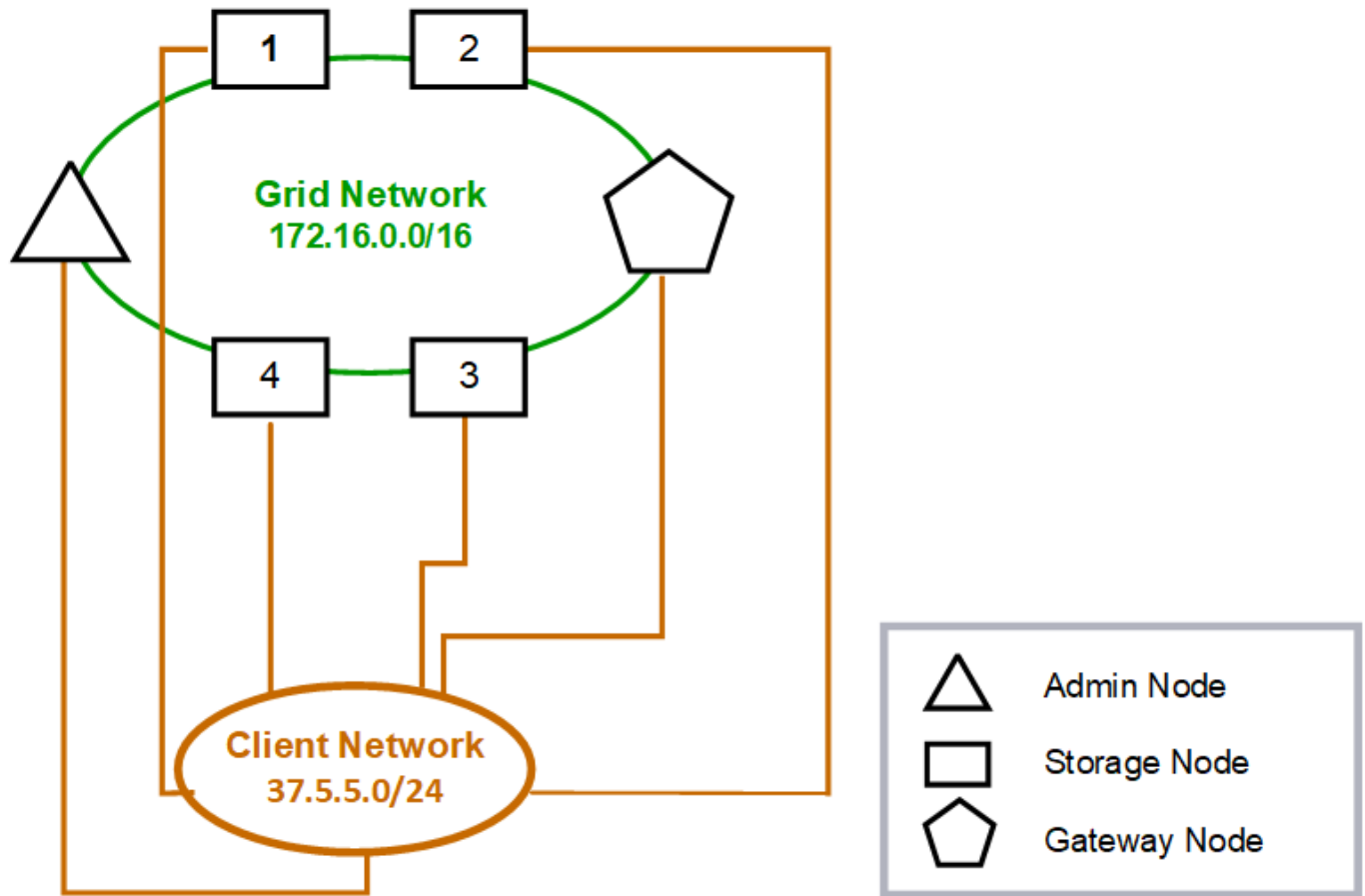
L'utilisation d'un réseau client est facultative. L'utilisation d'un réseau client permet de séparer le trafic réseau client (S3, par exemple) du trafic interne du grid, ce qui permet de sécuriser davantage le réseau grid. Le trafic administratif peut être géré par le client ou le réseau de grille lorsque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

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

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

Dans cet exemple, le réseau client est utilisé pour les requêtes des clients S3 et pour les fonctions administratives, tandis que le réseau Grid 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 associées

["Modifier la configuration réseau du nœud"](#)

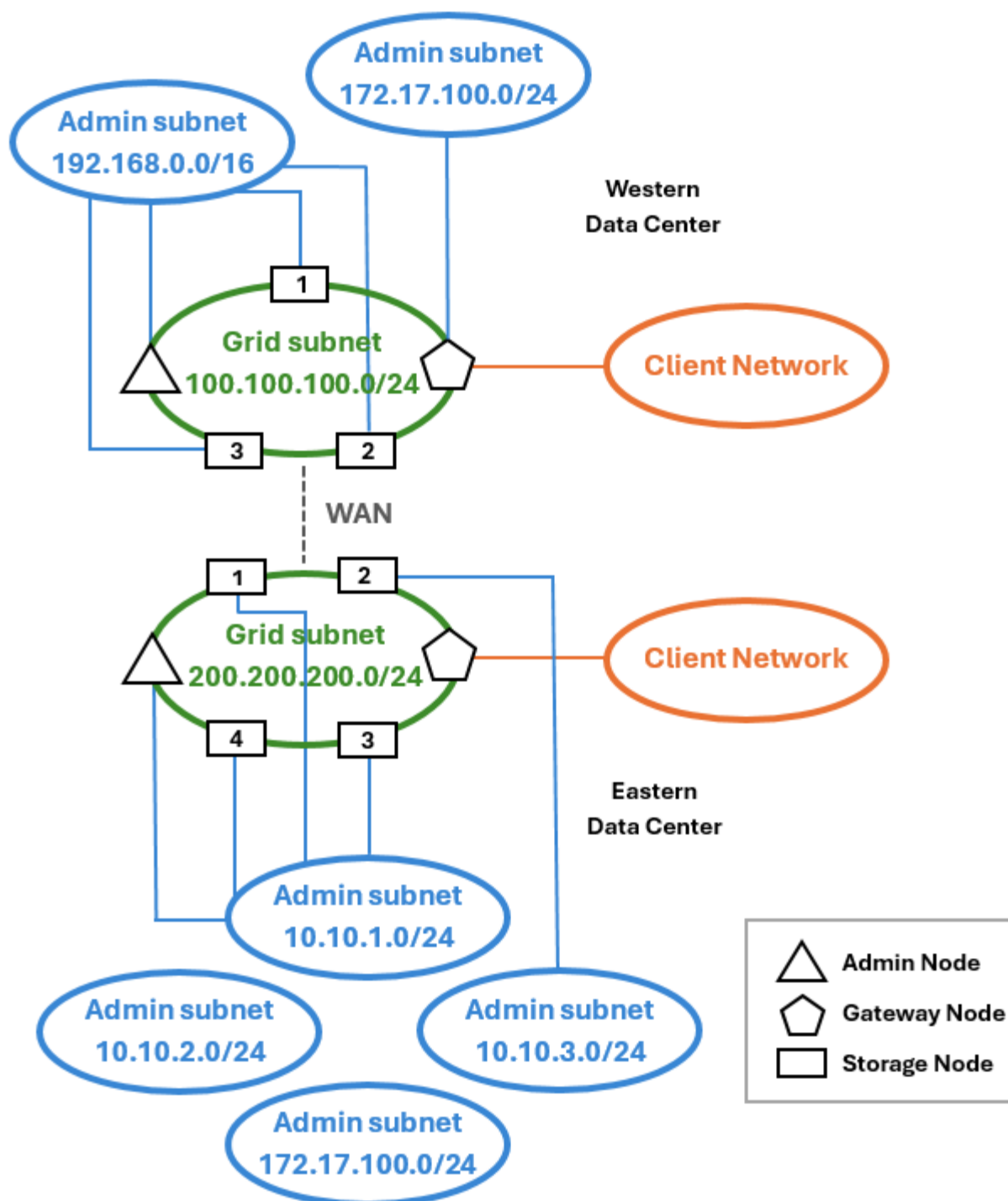
Topologie du réseau pour les trois réseaux StorageGRID

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

Dans cet exemple :

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

Exemple de topologie : réseaux Grid, Admin et client



Exigences réseau pour StorageGRID

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

Exigences générales de mise en réseau

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

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

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

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

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



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

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

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

Réseaux étendus (WAN) pour plusieurs sites

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

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

contactez votre consultant en services professionnels NetApp.

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

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

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

Utilisation de la traduction d'adresses réseau (NAT)

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

Exigences spécifiques au réseau pour StorageGRID

Respectez les exigences spécifiques à chaque type de réseau StorageGRID.

Passerelles et routeurs réseau

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

Sous-réseaux



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

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

- Le masque de sous-réseau d'une adresse IP réseau ne peut pas être 255.255.255.254 ou 255.255.255.255 (/31 ou /32 en notation CIDR).
- Le sous-réseau défini par une adresse IP d'interface réseau et un masque de sous-réseau (CIDR) ne peut pas chevaucher le sous-réseau d'une autre interface configurée sur le même nœud.
- 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

- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 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 du réseau Grid pour chaque nœud doit être inclus dans le GNSL.
- Le sous-réseau Admin Network ne peut pas chevaucher le sous-réseau Grid Network, le sous-réseau client Network ou tout sous-réseau dans le GNSL.
- Les sous-réseaux de l'AESL ne peuvent pas se chevaucher avec les sous-réseaux de la GNSL.
- Le sous-réseau du réseau client ne peut pas chevaucher le sous-réseau du réseau Grid, le sous-réseau du réseau Admin, tout sous-réseau du réseau GNSL ou tout sous-réseau de l'AESL.

Réseau Grid

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



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

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

Réseau d'administration

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

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



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



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

Réseau client

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

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

Informations associées

["Modifier la configuration réseau du nœud"](#)

Considérations relatives au réseau propres au déploiement

Configuration réseau pour les déploiements StorageGRID Linux

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

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



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

Voir le "[instructions d'installation](#)".

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

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

dispose de suffisamment de bande passante.

Hôtes physiques

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

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



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

- Ouvrez les ports requis vers l'hôte.
- Si vous prévoyez d'utiliser des interfaces VLAN dans StorageGRID, l'hôte doit disposer d'une ou plusieurs interfaces de jonction qui fournissent l'accès aux VLAN souhaités. Ces interfaces peuvent être transmises au conteneur de nœud comme eth0, eth2, ou comme interfaces supplémentaires. Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :
 - **Linux (avant l'installation du nœud):** ["Créez des fichiers de configuration de nœud"](#)
 - **Linux (après l'installation du nœud):** ["Ajouter des interfaces de jonction ou d'accès à un nœud"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#) .

Recommandations minimales sur la bande passante

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

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



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

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

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

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

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

Pour connaître certaines méthodes recommandées de configuration des ressources physiques et réseau sur les hôtes de votre cluster StorageGRID afin de préparer votre déploiement StorageGRID, consultez "[Configurez le réseau hôte](#)".

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

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

Mise en réseau pour les services de plate-forme

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

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

- Sur les nœuds de stockage avec services ADC, configurez des réseaux d'administration uniques avec des entrées AESL qui roulent vers les terminaux cibles.
- Utilisez la route par défaut fournie par un réseau client. Si vous utilisez l'itinéraire par défaut, vous pouvez utiliser "[Fonction 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 Microsoft Azure Blob Storage. 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 de pool de stockage cloud utilisent les ports suivants :

- **80** : pour les URI de point final commençant par `http`
- **443** : pour les URI de point final commençant par `https`

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

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

VLAN, services de plateforme et pools de stockage cloud

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

Configuration réseau pour les nœuds d'appliance StorageGRID

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

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

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

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

- "[Modes de liaison du port \(SG6160\)](#)"
- "[Modes de liaison du port \(SGF6112\)](#)"
- "[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 de port \(SG110 et SG1100\)](#)"
- "[Modes de liaison de port \(SG100 et SG1000\)](#)"

Installation et mise en service du réseau pour StorageGRID

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

Déploiement initial d'un nœud

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

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

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

Enregistrement automatique des nœuds avec le nœud d'administration principal

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

Désactivation du réseau Admin ou du réseau client

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

Consignes de post-installation pour StorageGRID

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

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

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



Les nœuds redémarrent lorsque la configuration Grid Network 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 Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un nœud de grille. Voir ["Configurez les adresses IP"](#).
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Référence du port réseau

Communications internes entre les nœuds de la grille pour StorageGRID

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



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

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

Instructions 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 des nœuds logiciels](#)".



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à "[Supprimez les mappes de ports sur les hôtes bare Metal](#)".

Instructions pour les nœuds VMware

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

Si les stratégies de 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 les instructions de "[installation de StorageGRID sur VMware](#)".



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à "[Supprimez les mappes de ports sur les hôtes bare Metal](#)".

Consignes pour les nœuds d'appliance

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



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à "[Supprimer les remappages de ports sur les appliances StorageGRID](#)".

Ports internes StorageGRID

Port	TCP ou UDP	De	À	Détails
22	TCP	Nœud d'administration principal	Tous les nœuds	Pour les procédures de maintenance, le nœud d'administration principal doit pouvoir communiquer avec tous les autres nœuds via SSH sur le port 22. L'autorisation du trafic SSH depuis d'autres nœuds est facultative.
80	TCP	Appliances	Nœud d'administration principal et nœud d'administration non principal	Utilisé par les appliances StorageGRID pour communiquer avec le nœud d'administration principal afin de démarrer l'installation.
123	UDP	Tous les nœuds	Tous les nœuds	Service de protocole de temps de réseau. Chaque nœud synchronise son heure avec chaque autre nœud à l'aide du protocole NTP.
443	TCP	Tous les nœuds	Nœud d'administration principal et nœud d'administration non principal	Utilisé pour communiquer l'état au nœud d'administration principal lors de l'installation et d'autres procédures de maintenance.
1055	TCP	Tous les nœuds	Nœud d'administration principal et nœud d'administration non principal	Trafic interne pour l'installation, l'extension, la récupération et d'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	Création de rapports, audit et configuration trafic interne.
1502	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne lié à S3.

Port	TCP ou UDP	De	À	Détails
1504	TCP	Tous les nœuds	Nœuds d'administration	Rapports de service NMS et trafic interne de configuration.
1505	TCP	Tous les nœuds	Nœuds d'administration	Trafic interne du service AMS.
1506	TCP	Tous les nœuds	Tous les nœuds	Trafic interne de l'état du serveur.
1507	TCP	Tous les nœuds	Nœuds de passerelle	Trafic interne de l'équilibreur de charge.
1508	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne de gestion de la configuration.
1511	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne de métadonnées.
5353	UDP	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. Remarque : La configuration de ce port est facultative.
7001	TCP	Nœuds de stockage	Nœuds de stockage	Communication inter-nœud Cassandra TLS avec cluster.
7443	TCP	Tous les nœuds	Nœud d'administration principal et nœud d'administration non principal	Trafic interne pour l'installation, l'extension, la récupération, les autres procédures de maintenance et le signalement des erreurs.

Port	TCP ou UDP	De	À	Détails
8011	TCP	Tous les nœuds	Nœud d'administration principal et nœud d'administration non principal	Trafic interne pour l'installation, l'extension, la récupération et d'autres procédures de maintenance.
8443	TCP	Nœud d'administration principal	Nœuds d'appliance	Trafic interne lié à la procédure de mode de maintenance.
9042	TCP	Nœuds de stockage	Nœuds de stockage	Port client Cassandra.
9999	TCP	Tous les nœuds	Tous les nœuds	Trafic interne pour plusieurs services. Inclut les procédures de maintenance, les mesures et les mises à jour réseau.
10226	TCP	Nœuds de stockage	Nœud d'administration principal	Utilisé par les appliances StorageGRID pour transférer les packages AutoSupport de E-Series SANtricity System Manager vers le nœud d'administration principal.
10342	TCP	Tous les nœuds	Nœud d'administration principal et nœud d'administration non principal	Trafic interne pour l'installation, l'extension, la récupération et d'autres procédures de maintenance.
18000	TCP	Tous les nœuds	Nœuds de stockage avec ADC	Trafic interne du service de compte.
18001	TCP	Tous les nœuds	Nœuds de stockage avec ADC	Trafic interne de la fédération des identités.
18002	TCP	Tous les nœuds	Nœuds de stockage	Trafic API interne lié aux protocoles objet

Port	TCP ou UDP	De	À	Détails
18003	TCP	Tous les nœuds	Nœuds de stockage avec ADC	Trafic interne des services de plate-forme.
18017	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic interne du service Data Mover pour les pools de stockage cloud.
18019	TCP	Tous les nœuds	Tous les nœuds	Trafic interne du service de fragmentation pour le codage d'effacement et la réplication
18082	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic interne lié à S3.
18086	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne lié au service LDR.
18200	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Statistiques supplémentaires sur les demandes client.
19000	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne du service Keystone.

Informations associées

["Communications externes"](#)

Communications externes pour StorageGRID

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

Accès restreint aux ports

Si les stratégies de mise en réseau d'entreprise limitent l'accès à l'un des ports, vous pouvez effectuer l'une des opérations suivantes :

- ["terminaux d'équilibrage de charge"](#) Permet d'autoriser l'accès aux ports définis par l'utilisateur.
- Remap les ports lors du déploiement des nœuds. Toutefois, vous ne devez pas remapper les terminaux de l'équilibreur de charge. Pour plus d'informations sur le remappage des ports pour votre nœud

StorageGRID, reportez-vous aux sections suivantes :



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à ["Supprimer les remappages de ports sur les appliances StorageGRID"](#) ou ["Supprimez les mappes de ports sur les hôtes bare Metal"](#).

- ["Clés de remap de port pour StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Remappez les ports pour StorageGRID sur VMware"](#)
- ["Facultatif : remappage des ports réseau pour l'appliance"](#)

Ports utilisés pour les communications externes

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



Cette liste n'inclut pas les ports qui peuvent être configurés comme ["terminaux d'équilibrage de charge"](#).

Port	TCP ou UDP	Protocole	De	À	Détails
22	TCP	SSH	L'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. Remarque : Ce port est uniquement requis lorsque vous devez activer l'accès SSH pour certaines opérations de maintenance.
25	TCP	SMTP	Nœuds d'administration	Serveur de messagerie	Utilisé pour les alertes et l'adresse AutoSupport basée sur des e-mails. Vous pouvez remplacer le paramètre de port par défaut de 25 à l'aide de la page serveurs de messagerie.
53	TCP/UDP	DNS	Tous les nœuds	Serveurs DNS	Utilisé pour DNS.
67	UDP	DHCP	Tous les nœuds	Service DHCP	Permet de prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne fonctionne pas pour les grilles configurées de façon statique.
68	UDP	DHCP	Service DHCP	Tous les nœuds	Permet de prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne s'exécute pas pour les grilles qui utilisent des adresses IP statiques.

Port	TCP ou UDP	Protocole	De	À	Détails
80	TCP	HTTP	Navigateur	Nœuds d'administration	Le port 80 redirige vers le port 443 pour l'interface utilisateur du nœud d'administration.
80	TCP	HTTP	Navigateur	Appliances	Le port 80 redirige vers le port 8443 du programme d'installation de l'appliance StorageGRID.
80	TCP	HTTP	Nœuds de stockage avec ADC	AWS	Utilisé pour les messages de services de plateforme envoyés à AWS ou à d'autres services externes utilisant HTTP. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la création d'un nœud final.
80	TCP	HTTP	Nœuds de stockage	AWS	Les demandes de pools de stockage cloud sont envoyées aux cibles AWS qui utilisent HTTP. Les administrateurs du grid peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la configuration d'un pool de stockage cloud.
123	UDP	NTP	Nœuds NTP principaux	NTP externe	Service de protocole de temps de réseau. Les nœuds sélectionnés comme sources NTP principales synchronisent également les heures d'horloge avec les sources d'heure NTP externes.
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. Le port UDP 161 est défini par défaut lorsqu'il est configuré. Remarque : ce port n'est nécessaire que, et n'est ouvert que sur le pare-feu de nœud si SNMP est configuré. Si vous prévoyez d'utiliser SNMP, vous pouvez configurer d'autres ports. Remarque : pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre ingénieur commercial NetApp.

Port	TCP ou UDP	Protocole	De	À	Détails
162	TCP/UDP	Notifications SNMP	Tous les nœuds	Destinations de notification	Notifications et interruptions SNMP sortantes par défaut au port UDP 162. Remarque : ce port n'est requis que si SNMP est activé et que les destinations de notification sont configurées. Si vous prévoyez d'utiliser SNMP, vous pouvez configurer d'autres ports. Remarque : pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre ingénieur commercial NetApp.
389	TCP/UDP	LDAP	Nœuds de stockage avec ADC	Active Directory/LDAP	Utilisé pour la connexion à un serveur Active Directory ou LDAP pour la fédération des identités.
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. Se référer à "Configurer les contrôles de pare-feu" pour configurer des adresses IP privilégiées.
443	TCP	HTTPS	Nœuds d'administration	Active Directory	Utilisé par les nœuds d'administration se connectant à Active Directory si l'authentification unique (SSO) est activée.
443	TCP	HTTPS	Nœuds de stockage avec ADC	AWS	Utilisé pour les messages de services de plateforme envoyés à AWS ou à d'autres services externes utilisant HTTPS. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 443 lors de la création d'un nœud final.
443	TCP	HTTPS	Nœuds de stockage	AWS	Les demandes de pools de stockage cloud sont envoyées aux cibles AWS qui utilisent HTTPS. Les administrateurs du grid peuvent remplacer le paramètre de port HTTPS par défaut de 443 lors de la configuration d'un pool de stockage cloud.

Port	TCP ou UDP	Protocole	De	À	Détails
636	TCP/UDP	LDAP	Nœuds de stockage avec ADC	Active Directory/LDAP	Utilisé pour la connexion à un serveur Active Directory ou LDAP pour la fédération des identités.
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. Remarque : La configuration de ce port est facultative.
5696	TCP	KMIP	Appliance	KM	Trafic externe KMIP (Key Management Interoperability Protocol) depuis les appliances configurées pour le chiffrement des nœuds vers le serveur de gestion des clés (KMS), sauf si un autre port est spécifié sur la page de configuration KMS du programme d'installation de l'appliance StorageGRID.
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, perdent l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées. Se référer à "Configurer les contrôles de pare-feu" pour configurer des adresses IP privilégiées.
8443	TCP	HTTPS	Navigateur	Appliances	Utilisé par les navigateurs Web et les clients API de gestion pour accéder au programme d'installation de l'appliance StorageGRID . Remarque : le port 443 redirige vers le port 8443 pour le programme d'installation de l'appliance StorageGRID .
9022	TCP	SSH	L'ordinateur portable de service	Appliances	Permet d'accéder aux appliances StorageGRID en mode préconfiguration pour le support et le dépannage. Ce port n'est pas nécessaire pour être accessible entre des nœuds grid ou pendant les opérations normales.

Port	TCP ou UDP	Protocole	De	À	Détails
9091	TCP	HTTPS	Service externe Grafana	Nœuds d'administration	Utilisés par les services Grafana externes pour sécuriser l'accès au service StorageGRID Prometheus. Remarque : ce port n'est nécessaire que si l'accès Prometheus basé sur un certificat est activé.
9092	TCP	Kafka	Nœuds de stockage avec ADC	Cluster Kafka	Utilisé pour les messages de services de plateforme envoyés à un cluster Kafka. Lors de la création d'un terminal, les locataires peuvent remplacer le paramètre par défaut du port Kafka 9092.
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).
18084	TCP	HTTP	Clients S3	Nœuds de stockage	Trafic client S3 directement vers les nœuds de stockage (HTTP).
23000-23999	TCP	HTTPS	Tous les nœuds du grid source pour la réplication inter-grid	Nœuds d'administration et nœuds de passerelle sur le grid de destination pour la réplication inter-grid	Cette plage de ports est réservée aux connexions de fédération de grille. Les deux grilles d'une connexion donnée utilisent le même port.

Démarrage rapide pour StorageGRID

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

1

Apprenez, planifiez et collectez des données

Contactez votre ingénieur commercial NetApp pour en savoir plus sur les options et planifier votre nouveau

système StorageGRID. Prenez en compte les types de questions suivants :

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

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

Examinez ["Découvrez StorageGRID"](#) et ["Instructions de mise en réseau"](#).

2

Installez les nœuds

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

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

Découvrez comment :

- ["Installez le matériel de l'appliance"](#)
- ["Installer StorageGRID sur des nœuds logiciels"](#)

3

Connectez-vous et vérifiez l'état du système

Une fois l'installation de la grille terminée, 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.

Découvrez comment :

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

4

Configuration et gestion

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

Découvrez comment :

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

5

Configuration d'ILM

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

Découvrez comment : ["Gestion des objets avec ILM"](#)

6

Utilisez StorageGRID

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

Découvrez comment :

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

7

Surveillance et résolution de problèmes

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

Découvrez comment :

- ["Surveillez StorageGRID"](#)
- ["Dépanner StorageGRID"](#)

8

Développez, entretenez et restaurez

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

Découvrez comment :

- "Développez une grille"
- "Maintenez votre grille"
- "Restaurer les nœuds"

Installez, mettez à niveau et correctif StorageGRID

Installer les nœuds StorageGRID

Découvrez le matériel des appliances StorageGRID

Accédez à "[Documentation de l'appliance StorageGRID](#)" pour savoir comment installer, configurer et maintenir les appliances de stockage et de services StorageGRID.

Installation des nœuds basés sur logiciel

Démarrage rapide pour l'installation de StorageGRID sur un nœud logiciel

Suivez ces étapes de haut niveau pour installer un nœud Linux ou VMware StorageGRID



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

1

Préparation

- En savoir plus sur "[Architecture StorageGRID et topologie réseau](#)".
- En savoir plus sur "[La mise en réseau StorageGRID](#)" les caractéristiques de .
- Rassembler et préparer le "[Informations et documents requis](#)".
- (VMware uniquement) Installer et configurer "[VMware vSphere Hypervisor, vCenter et les hôtes ESX](#)".
- Préparer le requis "[CPU et RAM](#)".
- Prévoir pour "[des besoins en termes de stockage et de performances](#)".
- (Linux uniquement) "[Préparez les serveurs Linux](#)" qui hébergera vos nœuds StorageGRID .

2

Déploiement

Déployez les nœuds grid. Lorsque vous déployez des nœuds grid, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.

- (Linux uniquement) 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](#)".
- (VMware uniquement) Utilisez le client Web VMware vSphere, un fichier .vmdk et un ensemble de modèles de fichiers .ovf pour "[Déploiement des nœuds logiciels en tant que machines virtuelles](#)" sur les serveurs que vous avez préparés à l'étape 1.
- Pour déployer des nœuds d'appliance StorageGRID, suivez la "[Démarrage rapide pour l'installation du matériel](#)".

Lorsque tous les nœuds ont été déployés, utilisez Grid Manager pour ["configurez la grille et terminez l'installation"](#).

Automatisez l'installation



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Linux

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

- Utilisez un framework d'orchestration standard comme Ansible, Puppet ou Chef pour l'automatisation :
 - Installation de Linux
 - Configuration du réseau et du stockage
 - Installation du moteur de mise en conteneurs et du service hôte StorageGRID
 - Déploiement de nœuds grid virtuels

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

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

VMware

Pour gagner du temps et assurer la cohérence, vous pouvez automatiser le déploiement et la configuration des nœuds du grid et de la configuration du système StorageGRID.

- ["Automatisez le déploiement des nœuds de grid à l'aide de VMware vSphere"](#).
- Après le déploiement de nœuds de grid ["Automatisez la configuration du système StorageGRID"](#) à l'aide du script de configuration Python fourni dans l'archive d'installation.
- ["Automatisation de l'installation et de la configuration des nœuds de grid des appliances"](#)
- Si vous êtes un développeur avancé de déploiements StorageGRID, automatisez l'installation des nœuds grid à l'aide de ["Installation de l'API REST"](#).

Planifier et préparer l'installation sur des nœuds basés sur des logiciels

Informations et documents requis pour StorageGRID

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

Informations requises

Plan du réseau

Réseaux que vous prévoyez de connecter à chaque nœud StorageGRID. StorageGRID prend en charge plusieurs réseaux pour la séparation du trafic, la sécurité et la facilité d'administration.

Consultez "[Instructions de mise en réseau](#)".

Informations sur le réseau

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

Serveurs pour nœuds grid

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



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

Migration de nœuds (Ubuntu et Debian uniquement, si nécessaire)

"[conditions requises pour la migration des nœuds](#)" Si vous souhaitez effectuer une maintenance planifiée sur des hôtes physiques sans interruption de service, consultez le .

Informations associées

"[Matrice d'interopérabilité NetApp](#)"

Matériel requis

Licence NetApp StorageGRID

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



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

Archive de l'installation de StorageGRID

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

L'ordinateur portable de service

Le système StorageGRID est installé par le biais d'un ordinateur portable de service.

L'ordinateur portable de service doit posséder :

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

Documentation StorageGRID

- "[Notes de mise à jour](#)". Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

- ["Instructions d'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. Vous pouvez également vérifier manuellement les fichiers du package d'installation.

Étapes

1. Accédez à la ["Page de téléchargements NetApp pour StorageGRID"](#).
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Si une instruction attention/MustRead apparaît, lisez-la et cochez la case.



Après l'installation de la version StorageGRID, vous devez appliquer les correctifs requis. Pour plus d'informations, reportez-vous à la section ["procédure de correctif dans les instructions de récupération et de maintenance"](#)

5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
6. Dans la colonne **Installer StorageGRID**, sélectionnez l'archive d'installation .tgz ou .zip pour votre type de nœud logiciel : RHEL, Ubuntu ou Debian, ou VMware.



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

7. Enregistrez l'archive d'installation.
8. La vérification de la signature du code est manuelle sur un nœud Linux. En option, 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 module 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 ["vérifiez manuellement les fichiers d'installation"](#).
9. Extrayez 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 planifiée et de la manière dont vous allez déployer votre système StorageGRID.



Les chemins répertoriés dans la table sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite.

RHEL

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Progiciel RPM pour l'installation des images de nœud StorageGRID sur vos hôtes RHEL.
	Progiciel RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle Ansible et de manuel de vente pour la configuration des hôtes RHEL pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Ubuntu ou Debian

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.

Chemin d'accès et nom de fichier	Description
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

VMware

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.

Chemin d'accès et nom de fichier	Description
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Le fichier modèle Open Virtualization format (.ovf) et le fichier manifeste (.mf) pour le déploiement du nœud d'administration principal.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement de nœuds Admin non primaires.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de passerelle.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.

Chemin d'accès et nom de fichier	Description
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Vérifier les fichiers d'installation de StorageGRID

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

Avant de commencer

Tu as ["téléchargez le pack de vérification - effectué"](#) de la ["Page de téléchargements NetApp pour StorageGRID"](#).

Étapes

1. Extraire les artefacts du progiciel de vérification :

```
tar -xf StorageGRID_12.1.0_Code_Signature_Verification_Package.tar.gz
```

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

- Certificat LEAF : `Leaf-Cert.pem`
- Chaîne de certificats : `CA-Int-Cert.pem`
- Chaîne de réponse avec horodatage : `TS-Cert.pem`
- Fichier checksum : `sha256sum`
- Signature du checksum : `sha256sum.sig`
- Fichier de réponse d'horodatage : `sha256sum.sig.tsr`

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

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

Sortie attendue : Leaf-Cert.pem: OK

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

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

La sortie attendue comprend : Verification: OK

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

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

Sortie attendue: None

6. Utilisez la clé publique pour vérifier le `sha256sum` fichier par rapport à `sha256sum.sig`.

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

Sortie attendue : Verified OK

7. Vérifiez `sha256sum` le contenu du fichier par rapport aux nouveaux checksums.

Exemple : `sha256sum -c sha256sum`

Sortie attendue: `<filename>: OK`

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

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

Exigences logicielles pour StorageGRID

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.

RHEL

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

Si vous sélectionnez une option d'installation de distribution Linux et d'exécution de conteneur qui nécessite 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 disponible auprès de votre fournisseur ou du fournisseur de support pour votre distribution Linux. Sinon, utilisez les versions de package par défaut disponibles auprès de votre fournisseur.

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



La prise en charge de Docker, car le moteur de mise en conteneurs pour les déploiements exclusivement logiciels est obsolète. Docker sera remplacé par un autre moteur de mise en conteneurs 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 Docker testées



La prise en charge de Docker est obsolète et sera supprimée dans une future 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

Ubuntu et Debian

Pour installer StorageGRID sur Ubuntu ou Debian, vous devez installer des paquets de logiciels tiers. Par défaut, certaines distributions Linux prises en charge ne contiennent pas ces packages. Les versions des progiciels sur lesquels les installations StorageGRID sont testées incluent celles répertoriées sur cette page.

Si vous sélectionnez une option d'installation de distribution Linux et d'exécution de conteneur qui nécessite 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 disponible auprès de votre fournisseur ou du fournisseur de support pour votre distribution Linux. Sinon, utilisez les versions de package par défaut disponibles auprès de votre fournisseur.

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



La prise en charge de Docker, car le moteur de mise en conteneurs pour les déploiements exclusivement logiciels est obsolète. Docker sera remplacé par un autre moteur de mise en conteneurs 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 Docker testées



La prise en charge de Docker est obsolète et sera supprimée dans une future 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

VMware

Hyperviseur VMware vSphere

Vous devez installer VMware vSphere Hypervisor sur un serveur physique préparé. Avant d'installer le logiciel VMware, le matériel doit être configuré correctement (y compris les versions du micrologiciel et les paramètres du BIOS).

- Configurez la mise en réseau dans l'hyperviseur pour prendre en charge la mise en réseau du système StorageGRID que vous installez.

["Instructions de mise en réseau"](#)

- Assurez-vous que le datastore est suffisamment grand pour les machines virtuelles et les disques virtuels requis pour héberger les nœuds de la grille.
- Si vous créez plusieurs datastores, nommez chacun d'entre eux afin de pouvoir facilement identifier les datastores à utiliser pour chaque nœud de la grille lorsque vous créez des machines virtuelles.

Exigences de configuration de l'hôte ESX



Vous devez configurer correctement le protocole NTP (Network Time Protocol) sur chaque hôte ESX. Si l'heure de l'hôte est incorrecte, des effets négatifs, y compris la perte de données, peuvent survenir.

Exigences de configuration 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 ["Matrice d'interopérabilité NetApp"](#).

Pour connaître les étapes d'installation de ces produits VMware, reportez-vous à la documentation VMware.

Exigences en matière de CPU et de RAM pour StorageGRID

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 au moins :

- Cœurs de processeur : 8 par nœud
- RAM : dépend de la mémoire 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
 - Si plusieurs locataires disposent chacun de jusqu'à 5 000 compartiments, au moins 64 Go par nœud



Le système StorageGRID prend en charge un maximum de 20 000 compartiments pour chaque compte locataire S3.

Les ressources de nœud exclusivement basées 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 exclusivement basés sur des métadonnées logicielles doivent respecter la configuration minimale suivante :
 - 128 GO DE RAM
 - Processeur 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 ; les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Linux

Vérifiez que le nombre de nœuds StorageGRID que vous prévoyez d'exécuter sur chaque hôte physique ou virtuel ne dépasse pas le nombre de cœurs de processeur ou la mémoire RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), veillez à prendre en compte les besoins en ressources des autres applications.

VMware

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 afin de garantir que ces ressources continuent de répondre à votre charge de travail. Par exemple, doubler la RAM et l'allocation de processeur 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 obtenir des informations sur la gestion du stockage des métadonnées d'objets, l'augmentation du paramètre Espace réservé aux métadonnées et la surveillance de l'utilisation du processeur et de la mémoire, consultez les instructions pour "[administration](#)", "[contrôle](#)" et "[mise à niveau](#)" StorageGRID.

Si le hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si le hyperthreading n'est pas activé sur les hôtes physiques sous-jacents, vous devez fournir 8 cœurs physiques par nœud.

Si vous utilisez des machines virtuelles en tant qu'hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, nous vous recommandons d'utiliser une seule machine virtuelle pour chaque nœud StorageGRID afin de dimensionner celle-ci en conséquence.

(RHEL, Debian et Ubuntu uniquement) 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.

Consultez "[Les besoins en matière de stockage et de performances](#)".

Exigences de stockage et de performance pour StorageGRID

Vous devez comprendre les exigences de stockage des nœuds StorageGRID afin de vous assurer que vous disposez de suffisamment d'espace pour prendre en charge la configuration initiale et les futures extensions de stockage.

Les exigences de stockage et de performances varient en fonction de l'implémentation de votre nœud basé sur un logiciel.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Catégories de stockage

Les nœuds StorageGRID nécessitent trois catégories logiques de stockage :

- **Pool de conteneurs** — Stockage de niveau performance (SAS 10K ou SSD) pour les conteneurs de nœud, qui est attribué au pilote de stockage du moteur de conteneurs lorsque vous installez et configurez le moteur de conteneurs sur les hôtes qui prennent en charge vos nœuds StorageGRID.
- **Données système** — Stockage de niveau performance (SAS 10K ou SSD) pour le stockage persistant par nœud des données système et des journaux de transactions, que les services hôtes StorageGRID consomment et mappent dans des nœuds individuels.
- **Données objet** — stockage de niveau performance (SAS 10 000 tr/min ou SSD) et stockage en bloc de niveau capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet et des métadonnées d'objet.

Vous devez utiliser des périphériques de blocs avec RAID pour toutes les catégories de stockage. Les disques non redondants, les SSD ou les JBOD ne sont pas pris en charge. Vous pouvez utiliser un stockage RAID partagé ou local pour toute catégorie de stockage. Pour migrer des nœuds dans StorageGRID, vous devez stocker à la fois les données système et les données d'objets sur un stockage partagé. Pour plus d'informations, consultez ["Exigences de migration des conteneurs de nœuds"](#).

Exigences en matière de performances

Les performances des volumes utilisés pour les pools de conteneurs, les données système et les métadonnées d'objet ont un impact significatif sur la performance globale du système. Pour ces volumes, il est recommandé d'utiliser un stockage de Tier de performances (SAS 10 000 tr/min ou SSD) pour garantir des performances de disque satisfaisantes en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit. Vous pouvez utiliser un stockage de niveau de capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet.

La mise en cache de l'écriture différée est activée sur les volumes utilisés pour le pool de conteneurs, les données système et les données d'objet. Le cache doit se trouver sur un support protégé ou persistant.

Exigences relatives aux hôtes qui utilisent un stockage NetApp ONTAP

Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Nombre d'hôtes requis

Chaque site StorageGRID requiert au moins trois nœuds de stockage.



En environnement de production, n'exécutez pas plus d'un nœud de stockage sur un même hôte physique ou virtuel. Un hôte dédié pour chaque nœud de stockage garantit un domaine de défaillance isolé.

Vous pouvez déployer d'autres types de nœuds, tels que des nœuds d'administration ou des nœuds de passerelle, sur les mêmes hôtes, ou vous pouvez les déployer sur leurs propres hôtes dédiés selon les besoins.



Il est impossible d'utiliser des instantanés de disque pour restaurer des nœuds de grille. Veuillez plutôt consulter les ["restauration du nœud grid"](#) procédures spécifiques à chaque type de nœud.

Nombre de volumes de stockage pour chaque nœud

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 déployés sur cet hôte.

La taille maximale de LUN testée est de 100 Tio.



Ces nombres sont pour chaque hôte, et non pour l'intégralité de la grille.

Objectif de LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Pool de stockage du moteur du conteneur	Pool de conteneurs	1	Nombre total de nœuds × 100 Go
/var/local volume	Données système	1 pour chaque nœud sur cet hôte	100 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 Linux et un nœud de stockage basé sur un logiciel VMware peuvent comporter de 1 à 48 volumes de stockage. Au moins 3 volumes de stockage sont recommandés.	12 To (4 To/LUN, minimum) Taille maximale du LUN testée : 100 Tio. Consultez Besoins de stockage des nœuds de stockage pour plus d'informations.
Nœud de stockage (métadonnées uniquement)	Métadonnées d'objet	1	4 To/LUN, minimum Taille maximale du LUN testée : 100 Tio. Consultez Besoins de stockage des nœuds de stockage pour plus d'informations. Remarque : un seul rangedb est requis pour les nœuds de stockage de métadonnées uniquement.

Objectif de LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Journaux d'audit du nœud d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO
Tables des nœuds d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO



Selon le niveau d'audit configuré, la taille des entrées utilisateur telles que le nom de la clé d'objet S3, et la quantité de données du journal des audits que vous devez conserver, il peut être nécessaire d'augmenter la taille du LUN du journal des audits 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 minimal 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 déployés sur cet hôte.



Il est impossible d'utiliser des instantanés de disque pour restaurer des nœuds de grille. Veuillez plutôt consulter les "[restauration du nœud grid](#)" procédures spécifiques à chaque type de nœud.

Chaque hôte de nœud nécessite un LUN de 100 Go pour le système d'exploitation.

Type de nœud	Pool de conteneurs	Données système	Données d'objet
Nœud de stockage	100 GO	100 GO	4,000 GO
Nœud d'administration	100 GO	500 Go (3 LUN)	<i>non applicable</i>
Nœud de passerelle	100 GO	100 GO	<i>non applicable</i>

Exemple : Calcul des besoins de stockage d'un hôte ou d'une machine virtuelle

Supposons que vous prévoyiez de déployer trois nœuds sur le même hôte ou machine virtuelle : un nœud de stockage, un nœud d'administration et un nœud de passerelle. Vous devez allouer au minimum neuf volumes de stockage à l'hôte. Il vous faut au minimum 300 Go de stockage hautes performances pour les conteneurs des nœuds, 700 Go de stockage hautes performances pour les données système et les journaux de transactions, et 12 To de stockage de capacité pour les données objets.

Exemple d'hôte Linux

Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud de stockage	Pool de stockage du moteur du conteneur	1	300 Go (100 Go/nœud)
Nœud de stockage	/var/local volume	1	100 GO
Nœud de stockage	Données d'objet	3	12 TO (4 TO/LUN)
Nœud d'administration	/var/local volume	1	100 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	100 GO
Total		9	Pool de conteneurs : 300 Go Données système : 700 Go Données d'objet : 12,000 Go

Exemple de machine virtuelle VMware

Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud de stockage	Volume du système d'exploitation	1	100 GO
Nœud de stockage	Données d'objet	3	12 TO (4 TO/LUN)
Nœud d'administration	Volume du système d'exploitation	1	100 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

Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud de passerelle	Volume du système d'exploitation	1	100 GO
Total		8	Données système : 700 Go Données d'objet : 12,000 Go

Exigences de stockage spécifiques pour les nœuds de stockage

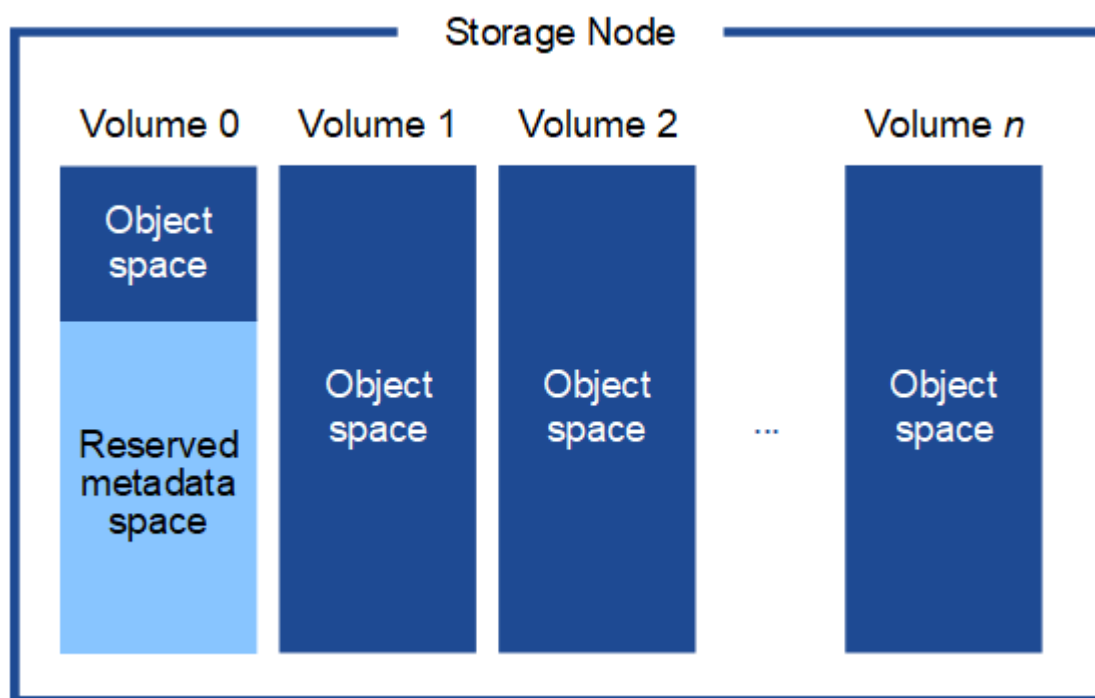
Linux et VMware ont les exigences de stockage suivantes pour les nœuds de stockage :

- Un nœud de stockage basé sur un logiciel Linux peut avoir de 1 à 48 volumes de stockage.
- Un nœud de stockage basé sur le logiciel VMware peut comporter de 1 à 48 volumes de stockage.
- Trois 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 illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tout autre volume de stockage du nœud de stockage est utilisé exclusivement pour les données d'objet.



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

Lors de l'installation d'une grille avec des nœuds de stockage dédiés aux métadonnées, la grille doit également comporter un nombre minimal de nœuds pour le stockage d'objets. Reportez-vous à ["Types de nœuds de stockage"](#) pour plus d'informations sur les nœuds de stockage dédiés aux métadonnées.

- Pour un grid à un seul site, 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 portion de ce nœud de toutes les métadonnées d'objet.

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



Si vous n'utilisez qu'un seul volume de stockage pour un nœud de stockage et que vous attribuez 4 To ou moins au volume, le nœud de stockage peut passer à l'état de stockage en lecture seule au démarrage et stocker uniquement les métadonnées d'objet.



Si vous attribuez moins de 500 Go au volume 0 (utilisation hors production uniquement), 10 % de la capacité du volume de stockage est réservée aux métadonnées.

- Les ressources de nœud exclusivement basées 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 exclusivement basés sur des métadonnées logicielles doivent respecter la configuration minimale suivante :
 - 128 GO DE RAM
 - Processeur 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 ; 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, si possible, le même paramètre pour le volume 0. Si un site contient des nœuds de stockage de tailles différentes, le nœud de stockage avec le plus petit volume 0 détermine la capacité de métadonnées de ce site.

Pour plus de détails, rendez-vous sur ["Gérer le stockage des métadonnées d'objet"](#).

Exigences de migration des conteneurs de nœuds StorageGRID pour Linux

La fonction de migration de nœud vous permet de déplacer manuellement un nœud d'un

hôte à un autre. En général, les deux hôtes se trouvent dans le même data Center physique.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

La migration des nœuds vous permet d'effectuer la maintenance des hôtes physiques sans interrompre les opérations de la grille. Vous déplacez tous les nœuds StorageGRID, un par un, vers un autre hôte avant de mettre l'hôte physique hors ligne. La migration de nœuds ne demande qu'une interruption courte pour chaque nœud et ne doit en aucun cas affecter le fonctionnement ou la disponibilité des services de grid.

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

- Noms d'interface réseau cohérents entre les hôtes dans un seul data Center physique
- Stockage partagé pour les métadonnées StorageGRID et les volumes de référentiel d'objets accessibles par tous les hôtes dans un seul data Center physique. Vous pouvez, par exemple, utiliser des baies de stockage NetApp E-Series.

Si vous utilisez des hôtes virtuels et que la couche de l'hyperviseur sous-jacent prend en charge la migration des ordinateurs virtuels, vous pouvez utiliser cette fonctionnalité à la place de la fonctionnalité de migration des nœuds de StorageGRID. Dans ce cas, vous pouvez ignorer ces exigences supplémentaires.

Avant d'effectuer la migration ou la maintenance de l'hyperviseur, arrêtez les nœuds selon les besoins. Voir les instructions pour ["arrêt d'un nœud grid"](#).

VMware Live migration non pris en charge

Lors d'une installation sans système d'exploitation sur des machines virtuelles VMware, OpenStack Live migration et VMware Live vMotion entraînent un bond de l'horloge de la machine virtuelle et ne sont pas pris en charge pour les nœuds de grid, quel qu'en soit le type. Bien que les temps d'horloge rares et incorrects peuvent entraîner une perte de données ou des mises à jour de la configuration.

La migration à froid est prise en charge. Dans le cadre d'une migration à froid, vous devez arrêter les nœuds StorageGRID avant de les migrer entre les hôtes. Voir les instructions pour ["arrêt d'un nœud grid"](#).

Noms d'interface réseau cohérents

Pour déplacer un nœud d'un hôte à un autre, le service d'hôte StorageGRID doit être certain que la connectivité réseau externe du nœud à son emplacement actuel peut être dupliquée au nouvel emplacement. Cette confiance est obtenue grâce à l'utilisation de noms d'interface réseau cohérents dans les hôtes.

Supposons, par exemple, que le nœud StorageGRID exécutant sur Host1 ait été configuré avec les mappages d'interface suivants :

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Le côté gauche des flèches correspond aux interfaces traditionnelles affichées à partir d'un conteneur StorageGRID (c'est-à-dire, respectivement, les interfaces réseau Grid, Admin et client). Le côté droit des flèches correspond aux interfaces hôtes réelles fournissant ces réseaux, qui sont trois interfaces VLAN subordonnées à la même liaison d'interface physique.

Supposons maintenant que vous voulez migrer NodeA vers Host2. Si Host2 possède également des interfaces nommées bond0.1001, bond0.1002, et bond0.1003, le système permettra le déplacement, en supposant que les interfaces nommées similaires fourniront la même connectivité sur Host2 que sur Host1. Si Host2 ne possède pas d'interfaces avec les mêmes noms, le déplacement ne sera pas autorisé.

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

Stockage partagé

Pour réaliser des migrations de nœuds rapides et sans surcharge, la fonctionnalité de migration de nœuds StorageGRID ne déplace pas physiquement les données du nœud. La migration des nœuds se déroule comme une paire d'opérations d'exportation et d'importation :

- Lors de l'opération d'exportation de nœud, une petite quantité de données d'état persistant est extraite du conteneur de nœud s'exécutant sur HostA et mise en cache sur le volume de données système de ce nœud. Ensuite, le conteneur de nœud sur HostA est déinstancié.
- Lors de l'opération d'importation de nœud, le conteneur de nœud sur l'hôte B qui utilise les mêmes mappages de mémoire de bloc et d'interface réseau qui étaient en vigueur sur l'hôte A est instancié. Les données de l'état persistant en cache sont ensuite insérées dans la nouvelle instance.

Compte tenu de ce mode de fonctionnement, toutes les données système et les volumes de stockage objet du nœud doivent être accessibles à la fois à HostA et HostB pour que la migration soit autorisée, et pour fonctionner. En outre, ils doivent avoir été mappés dans le nœud en utilisant des noms qui sont garantis pour faire référence aux mêmes LUN sur HostA et HostB.

L'exemple suivant montre une solution pour le mappage de périphériques en mode bloc pour un nœud de stockage StorageGRID, où les chemins d'accès multiples DM sont utilisés sur les hôtes, et le champ alias a été utilisé dans `/etc/multipath.conf` pour fournir des noms de périphériques en mode 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 (Linux)

Comment StorageGRID modifie les paramètres globaux de l'hôte

Sur les systèmes bare Metal, StorageGRID modifie les paramètres de l'hôte `sysctl`.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

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 StorageGRID sur des hôtes de grille Linux

Vous devez installer StorageGRID sur tous les hôtes de grille 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 StorageGRID en matière de version du noyau, comme indiqué ci-dessous. Utilisez la commande `uname -r` pour obtenir la version du noyau de votre système d'exploitation ou consultez votre fournisseur de système d'exploitation.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

RHEL

Version RHEL	Version minimale du noyau	Nom du package du noyau
8.8 (obsolète)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8.10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 (obsolète)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 (obsolète)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-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

Ubuntu

Note: le support pour Ubuntu versions 18.04 et 20.04 ont été dépréciés et seront supprimés dans une future version.

Version Ubuntu	Version minimale du noyau	Nom du package du noyau
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

Debian

Note: le support de Debian version 11 est obsolète et sera supprimé dans une version ultérieure.

Version de Debian	Version minimale du noyau	Nom du package 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 réseau physiques ou virtuels conformément aux instructions du distributeur ou à la procédure standard.



N'installez aucun environnement de bureau graphique.

- Si vous utilisez le programme d'installation Linux standard lors de l'installation de RHEL, sélectionnez la configuration logicielle « nœud de calcul », si disponible, ou l'environnement de base « installation minimale ».
 - 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, y compris le canal Extras pour RHEL.
 3. Si le swap est activé :
 - a. Exécutez la commande suivante : `$ sudo swapoff --all`
 - b. Supprimez toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.



Si vous ne désactivez pas ces fichiers, les performances peuvent être considérablement réduites.

Découvrez les profils AppArmor pour StorageGRID sur Ubuntu et Debian

Si vous travaillez dans un environnement Ubuntu déployé automatiquement et que vous utilisez le système de contrôle d'accès obligatoire AppArmor, il est possible que les profils AppArmor associés aux paquets que vous installez sur le système de base soient bloqués par les paquets correspondants installés avec StorageGRID.

Par défaut, les profils AppArmor sont installés pour les packages que vous installez sur le système d'exploitation de base. Lorsque vous exécutez ces packages à partir du conteneur système StorageGRID, les profils AppArmor sont bloqués. Les paquets de base DHCP, MySQL, NTP et tcdump sont en conflit avec AppArmor, et d'autres paquets de base peuvent également entrer en conflit.

Vous avez le choix entre deux options pour gérer les profils AppArmor :

- Désactivez les profils individuels pour les packages installés sur le système de base qui se chevauchent avec les packages du conteneur système StorageGRID. Lorsque vous désactivez des profils individuels, une entrée apparaît dans les fichiers journaux StorageGRID indiquant qu'AppArmor est activé.

Utiliser les commandes suivantes :

```
sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
```

Exemple:

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- Désactivez complètement AppArmor. Pour Ubuntu 9.10 ou version ultérieure, suivez les instructions dans le ["Communauté en ligne Ubuntu"](#). La désactivation complète de AppArmor peut ne pas être possible sur les versions plus récentes d'Ubuntu.

Après avoir désactivé AppArmor, aucune entrée indiquant que AppArmor est activé n'apparaît dans les fichiers journaux StorageGRID.

Configurer le réseau hôte StorageGRID pour les déploiements Linux

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être procéder à une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte, adapté au mappage vers les nœuds StorageGRID que vous pourrez déployer ultérieurement.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Avant de commencer

- Vous avez consulté les informations dans ["Instructions de mise en réseau"](#).
- 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 relatives au clonage d'adresses MAC](#) avant de configurer le réseau hôte.



Si vous utilisez des machines virtuelles en tant qu'hôtes, vous devez sélectionner VMXNET 3 comme carte réseau virtuelle. La carte réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

Description de la tâche

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

Une même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès aux hôtes et l'accès au réseau d'administration de nœud afin de faciliter la maintenance des hôtes et des nœuds. Même si une même interface peut être partagée entre l'hôte et les nœuds individuels, toutes doivent avoir des adresses IP différentes. Les adresses IP ne peuvent pas être partagées entre les nœuds ou entre l'hôte et un nœud.

Vous pouvez utiliser la même interface réseau hôte pour fournir l'interface réseau Grid de tous les nœuds StorageGRID de l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou effectuer un travail entre les deux. Cependant, vous ne fournissez généralement pas la même interface réseau hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou l'interface réseau Grid pour un nœud et l'interface réseau client pour un autre.

Vous pouvez effectuer cette tâche de plusieurs manières. Par exemple, si vos hôtes sont des machines virtuelles et que vous déployez un ou deux nœuds StorageGRID pour chaque hôte, vous pouvez créer le nombre correct d'interfaces réseau dans l'hyperviseur et utiliser un mappage 1-to-1. Si vous déployez plusieurs nœuds sur des hôtes bare Metal pour la production, vous pouvez bénéficier de la prise en charge du VLAN et du LACP de la pile réseau Linux pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes présentent des approches détaillées pour ces deux exemples. Vous n'avez pas besoin

d'utiliser l'un ou l'autre de ces exemples ; vous pouvez utiliser n'importe quelle approche qui répond à vos besoins.



N'utilisez pas de périphérique de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage de nœud causé par un problème de noyau avec l'utilisation de MACVLAN avec des périphériques de liaison et de pont dans l'espace de noms de conteneur. Utilisez plutôt un périphérique sans lien, tel qu'un VLAN ou une paire Ethernet virtuelle (Veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration de nœud.

Considérations et recommandations relatives au clonage d'adresses MAC

Le clonage d'adresse MAC permet au conteneur d'utiliser l'adresse MAC de l'hôte, et à l'hôte d'utiliser l'adresse MAC soit d'une adresse que vous spécifiez, soit d'une adresse générée aléatoirement.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être renforcée grâce au clonage d'adresses MAC, car cela vous permet d'utiliser une carte réseau virtuelle dédiée pour le Admin Network, le Grid Network et le Client Network.



Le clonage d'adresses MAC est conçu pour être utilisé avec des installations de serveurs virtuels et peut ne pas fonctionner correctement avec toutes les configurations d'appliances physiques.



Si un nœud ne démarre pas en raison d'une interface ciblée de clonage MAC occupée, il peut être nécessaire de définir le lien sur « down » avant de démarrer le nœud. En outre, il est possible que l'environnement virtuel puisse empêcher le clonage MAC sur une interface réseau pendant que la liaison est active. Si un nœud ne parvient pas à définir l'adresse MAC et démarre en raison d'une interface en cours d'activité, il est possible que le problème soit résolu en définissant le lien sur « arrêté » avant de démarrer le nœud.

Le clonage d'adresses MAC est désactivé par défaut et doit être défini par des clés de configuration de nœud. Vous devez l'activer lors de l'installation de StorageGRID.

Il existe une clé pour chaque réseau :

- ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Le fait de définir la clé sur « true » fait que le conteneur utilise l'adresse MAC de la carte réseau de l'hôte. En outre, l'hôte utilisera ensuite l'adresse MAC du réseau de conteneurs spécifié. Par défaut, l'adresse du conteneur est une adresse générée de manière aléatoire, mais si vous en avez défini une à l'aide de la `_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.

Cas d'utilisation du clonage MAC

Il existe deux cas d'utilisation à prendre en compte pour le clonage MAC :

- Clonage MAC désactivé : lorsque la clé `_CLONE_MAC` dans le fichier de configuration du nœud n'est pas définie ou est définie sur « false », l'hôte utilisera la MAC de la carte réseau de l'hôte et le conteneur aura une MAC générée par StorageGRID, sauf si une MAC est spécifiée dans la clé `_NETWORK_MAC`. Si une adresse est définie dans la clé `_NETWORK_MAC`, le conteneur aura l'adresse spécifiée dans la clé `_NETWORK_MAC`.
- Clonage MAC activé : lorsque la clé `_CLONE_MAC` dans le fichier de configuration du nœud est définie sur « true », le conteneur utilise la MAC de la carte réseau de l'hôte et l'hôte utilise une MAC générée par StorageGRID, sauf si une MAC est spécifiée dans la clé `_NETWORK_MAC`. Si une adresse est définie dans la clé `_NETWORK_MAC`, l'hôte utilise l'adresse spécifiée au lieu d'une adresse générée.



Si vous ne souhaitez pas utiliser le clonage d'adresses 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 les modifications d'adresses MAC et les transmissions falsifiées. Les valeurs définies au niveau du commutateur virtuel peuvent être remplacées par celles définies au niveau du groupe de ports, alors assurez-vous que les paramètres soient identiques aux deux endroits.

Pour activer le clonage MAC, reportez-vous au ["instructions pour la création de fichiers de configuration de nœud"](#).

Exemple de clonage MAC

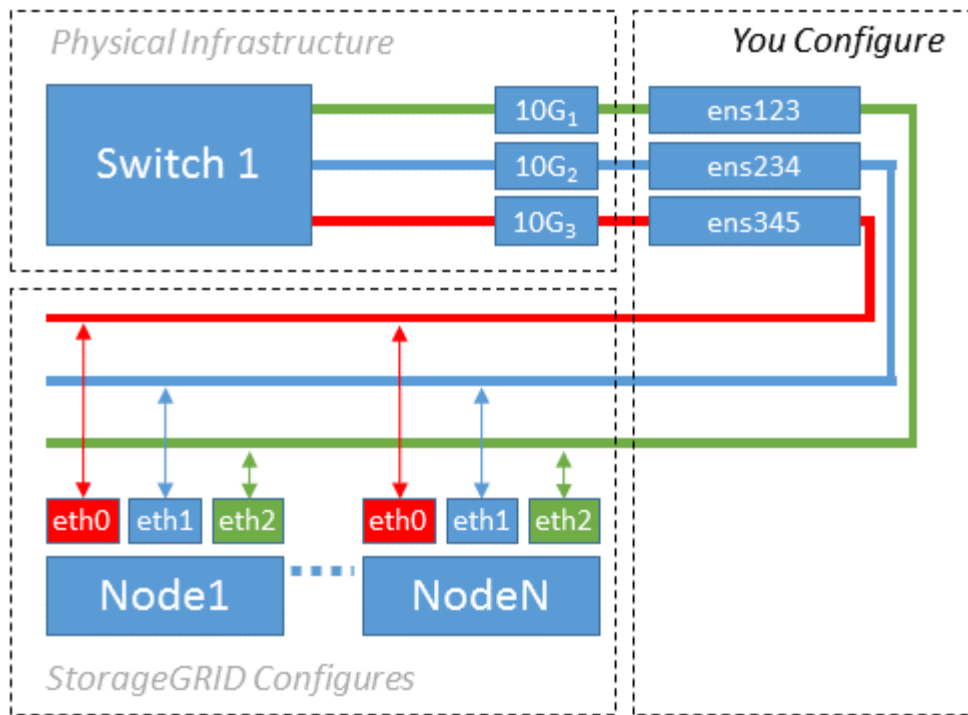
Exemple de clonage MAC activé avec un hôte dont l'adresse MAC est 11:22:33:44:55:66 pour le groupe d'interface 256 et les clés suivantes dans le fichier de configuration de nœud :

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

Résultat: L'hôte MAC pour en256 est b2:9c:02:c2:27:10 et l'Admin réseau MAC est 11:22:33:44:55:66

Exemple 1 : mappage 1-à-1 sur des cartes réseau physiques ou virtuelles

L'exemple 1 décrit un mappage d'interface physique simple qui nécessite peu ou pas de configuration côté hôte.



Le système d'exploitation Linux crée le `ensXYZ` interfaces automatiquement lors de l'installation ou du démarrage, ou lorsque les interfaces sont ajoutées à chaud. Aucune configuration n'est 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 présente plusieurs nœuds StorageGRID. Toutefois, vous utilisez généralement cette configuration pour les machines virtuelles à un seul nœud.

Si le commutateur 1 est un commutateur physique, vous devez configurer les ports connectés aux interfaces 10G1 à 10G3 pour le mode d'accès et les placer sur les VLAN appropriés.

Exemple 2 : liaison LACP avec les VLAN

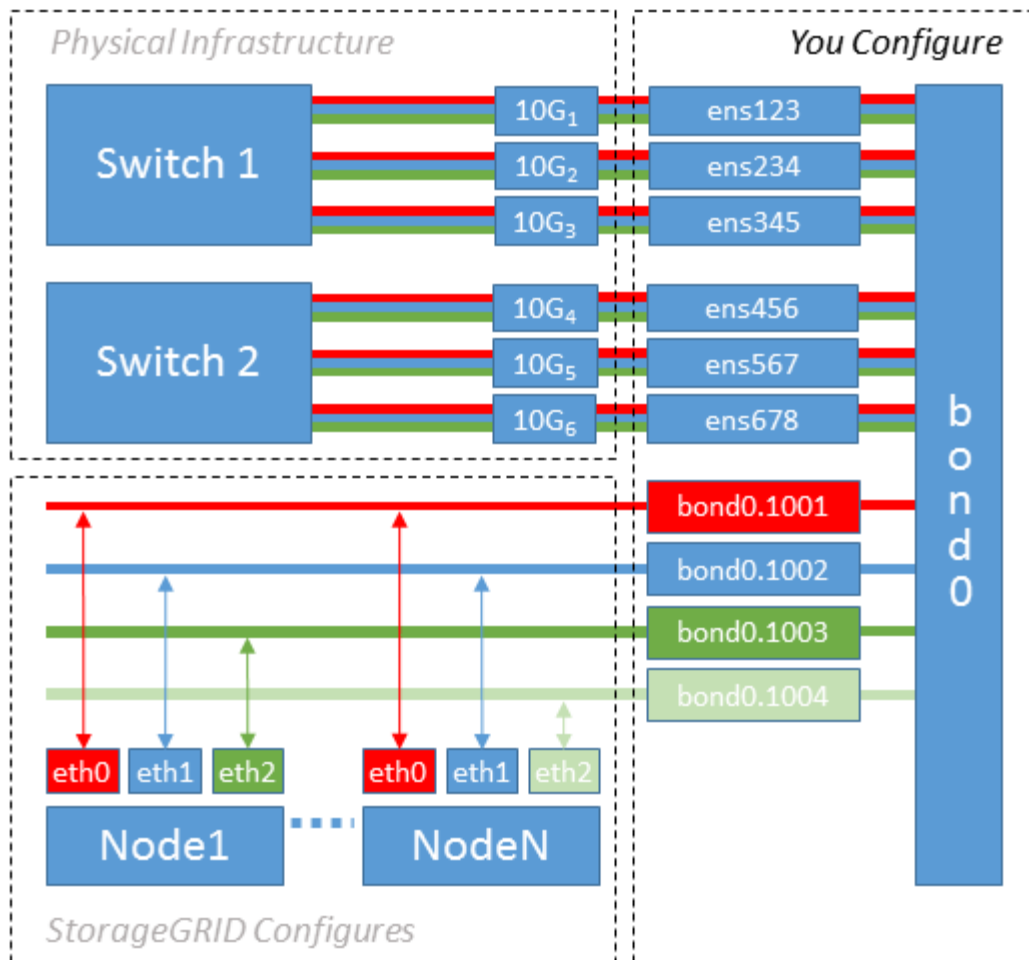
L'exemple 2 suppose que vous êtes familier avec les interfaces réseau de liaison et avec la création d'interfaces VLAN sur la distribution Linux que vous utilisez.

Description de la tâche

L'exemple 2 décrit un schéma générique, flexible et basé sur VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un même hôte. Cet exemple s'applique tout particulièrement aux hôtes bare Metal.

Pour comprendre cet exemple, supposons que vous ayez trois sous-réseaux distincts pour les réseaux Grid, Admin et client dans chaque centre de données. Les sous-réseaux se trouvent sur des VLAN distincts (1001, 1002 et 1003) et sont présentés à l'hôte sur un port de jonction lié à LACP (`bond0`). Vous devez configurer trois interfaces VLAN sur la liaison : `bond0.1001`, `bond0.1002` et `bond0.1003`.

Si vous avez besoin de VLAN et de sous-réseaux distincts pour les réseaux de nœuds sur le même hôte, vous pouvez ajouter des interfaces VLAN sur la liaison et les mapper sur l'hôte (voir `bond0.1004` dans l'illustration).



Étapes

1. Agréger toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID en une seule liaison LACP.

Utilisez le même nom pour le lien sur chaque hôte, par exemple, `bond0`.

2. Créez des interfaces VLAN qui utilisent cette liaison comme « périphérique physique » associé, 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 qui terminent les autres extrémités des liaisons réseau. Les ports de switch de périphérie doivent également être agrégés dans un canal de port LACP, configuré en tant que jonction et autorisé à passer tous les VLAN requis.

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

Informations associées

- ["Exemple de /etc/network/interfaces pour Ubuntu et Debian"](#)
- ["Exemple de scripts /etc/sysconfig/network-scripts pour RHEL"](#)

Configurer le stockage hôte StorageGRID pour les déploiements Linux

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

Avant de commencer

Vous avez passé en revue les sujets suivants, qui fournissent les informations nécessaires pour accomplir cette tâche :

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



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Description de la tâche

Lors de l'allocation de volumes de stockage en mode bloc (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 à déployer sur cet hôte)
- Catégorie de stockage pour chaque volume (données système ou données objet)
- Taille de chaque volume

Lors du déploiement de nœuds StorageGRID sur l'hôte, vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique.



Il n'est pas nécessaire de partitionner, de formater ou de monter ces volumes ; il vous suffit de vous assurer qu'ils sont visibles par les hôtes.



Pour les nœuds de stockage des métadonnées uniquement, un seul LUN de données d'objet est requis.

Évitez d'utiliser des fichiers de périphérique spéciaux "bruts" (`/dev/sdb`, par exemple) lorsque vous composez votre liste de noms de volume. Ces fichiers peuvent être modifiés entre les redémarrages de l'hôte, ce qui peut affecter le fonctionnement correct du système. Si vous utilisez des LUN iSCSI et des chemins d'accès multiples de Device Mapper, envisagez d'utiliser des alias de chemins d'accès multiples dans le `/dev/mapper` répertoire, surtout si votre topologie SAN inclut des chemins réseau redondants vers le stockage partagé. Vous pouvez également utiliser les liens logiciels créés par le système sous `/dev/disk/by-path/` pour les noms de vos périphériques persistants.

Par exemple :

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Les résultats diffèrent pour chaque installation.

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

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 façon entraîne l'affichage des alias en tant que périphériques de bloc dans le `/dev/mapper` répertoire de l'hôte, ce qui vous permet 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 de bloc.

Si vous configurez un stockage partagé pour prendre en charge la migration des nœuds StorageGRID et que vous utilisez le multipathing du mappeur de périphériques, vous pouvez créer et installer une connexion commune `/etc/multipath.conf` sur tous les hôtes en colocation. Veillez à utiliser un volume de stockage moteur de mise en conteneurs différent sur chaque hôte. L'utilisation d'alias et l'inclusion du nom d'hôte cible dans l'alias pour chaque LUN de volume de stockage de moteur de conteneur rendent cela facile à mémoriser et est recommandé.



La prise en charge de Docker, car le moteur de mise en conteneurs pour les déploiements exclusivement logiciels est obsolète. Docker sera remplacé par un autre moteur de mise en conteneurs dans une prochaine version.

Informations associées

- ["Configurer le volume de stockage du moteur du conteneur"](#)
- ["Les besoins en matière de stockage et de performances"](#)
- ["Exigences de migration des conteneurs de nœuds"](#)

Configurer le volume de stockage du moteur de conteneur pour StorageGRID sur Linux

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, car le moteur de mise en conteneurs pour les déploiements exclusivement logiciels est obsolète. Docker sera remplacé par un autre moteur de mise en conteneurs dans une prochaine version.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Description de la tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser le volume racine pour le volume de stockage Docker ou Podman et que vous disposez de suffisamment d'espace disponible sur la partition hôte contenant :

- Podman : `/var/lib/containers`
- Docker : `/var/lib/docker`

Étapes

1. Créer un système de fichiers sur le volume de stockage du moteur de conteneur :

RHEL

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

Ubuntu ou Debian

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Monter le volume de stockage du moteur du conteneur :

RHEL

- 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
```

Ubuntu ou Debian

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

- Pour Podman :

```
sudo mkdir -p /var/lib/podman
sudo mount container-storage-volume-device /var/lib/podman
```

3. Ajoutez une entrée pour le périphérique de volume de stockage du conteneur dans /etc/fstab.

- RHEL : conteneur-volume-de-stockage-périphérique
- Ubuntu ou Debian : docker-storage-volume-device

Cette étape permet de s'assurer que le volume de stockage se réajuste automatiquement après le redémarrage de l'hôte.

Installez Docker

Le système StorageGRID peut fonctionner sous Linux en tant que collection de conteneurs.

- Avant de pouvoir installer StorageGRID pour Ubuntu ou Debian, vous devez installer Docker.
- Si vous avez choisi d'utiliser le moteur de conteneur Docker, suivez ces étapes pour installer Docker. Sinon, [Installez Podman](#) .



La prise en charge de Docker, car le moteur de mise en conteneurs pour les déploiements exclusivement logiciels est obsolète. Docker sera remplacé par un autre moteur de mise en conteneurs 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 sur le site Web de Docker.

2. Assurez-vous que Docker a été activé et démarré en exécutant les deux commandes suivantes :

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Vérifiez que vous avez installé la version attendue de Docker en saisissant les éléments suivants :

```
sudo docker version
```

Les versions client et serveur doivent être 1.11.0 ou supérieures.

Installez Podman

Le système StorageGRID fonctionne comme une collection de conteneurs. Si vous avez choisi d'utiliser le moteur de conteneur Podman, suivez ces étapes pour installer Podman. Sinon, [Installez Docker](#) .

Étapes

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



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

2. Vérifiez que vous avez installé la version attendue de Podman et Podman-Docker en saisissant les éléments suivants :

```
sudo docker version
```



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

Les versions client et serveur doivent être 3.2.3 ou supérieures.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Informations associées

["Configurer le stockage de l'hôte"](#)

Installer les services hôtes StorageGRID sous Linux

Vous utilisez le package StorageGRID pour votre type de système d'exploitation pour installer les services hôtes StorageGRID .



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#) .

RHEL

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

Description de la tâche

Ces instructions décrivent l'installation des services hôtes à partir des packages RPM. Vous pouvez également utiliser les métadonnées du référentiel 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 mettez-les à disposition sur un stockage partagé.

Par exemple, placez-les dans le `/tmp` répertoire pour pouvoir 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 et le package Service en second.



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

Ubuntu ou Debian

Vous utilisez le package DEB StorageGRID pour installer les services hôtes StorageGRID pour Ubuntu ou Debian.

Description de la tâche

Ces instructions décrivent l'installation des services hôtes à partir des packages DEB. Vous pouvez également utiliser les métadonnées du référentiel APT incluses dans l'archive d'installation pour installer les packages DEB à distance. Consultez les instructions du référentiel APT pour votre système d'exploitation Linux.

Étapes

1. Copiez les packages DEB StorageGRID sur chacun de vos hôtes, ou mettez-les à disposition sur un stockage partagé.

Par exemple, placez-les dans le `/tmp` répertoire pour pouvoir 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 d'abord installer le `images` package, puis le `service` package. Si vous avez placé les modules 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 3 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.

Automatisez l'installation des nœuds logiciels

Automatisez l'installation du service hôte StorageGRID et la configuration des nœuds de la grille sous Linux

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



Description de la tâche

« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

L'automatisation du déploiement peut être utile dans les cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, comme Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.
- Vous prévoyez de déployer plusieurs instances StorageGRID.
- Vous déployez une instance StorageGRID vaste et complexe.

Le service hôte StorageGRID est installé par un package et piloté par des fichiers de configuration. Vous pouvez créer les fichiers de configuration à l'aide de l'une des méthodes suivantes :

- ["Créez les fichiers de configuration"](#) interactivement pendant une installation manuelle.
- Préparez les fichiers de configuration à l'avance (ou par programmation) pour permettre une installation automatisée à l'aide des frameworks d'orchestration standard, comme le décrit dans cet article.

StorageGRID propose des scripts Python en option pour l'automatisation de la configuration des appliances StorageGRID et de l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement ou les examiner pour apprendre à utiliser les outils de déploiement et de configuration du ["API REST d'installation de StorageGRID"](#) grid que vous développez vous-même.

Automatisez l'installation et la configuration du service d'hôte StorageGRID

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

Le service hôte StorageGRID est conditionné dans un DEB (Ubuntu ou Debian) ou un RPM (RHEL) 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 votre déploiement Linux, l'ajout de StorageGRID à vos playbooks ou recettes devrait être simple.

Vous pouvez automatiser toutes les étapes pour préparer les hôtes et déployer des nœuds de grille virtuels.

Exemple de rôle et de PlayBook Ansible

Un exemple de rôle Ansible et de PlayBook sont fournis avec l'archive d'installation dans le `/extras` dossier. Ce PlayBook explique comment le `storagegrid` rôle prépare les hôtes et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.



Le PlayBook exemple n'inclut pas les étapes requises pour créer des périphériques réseau avant de démarrer le service hôte StorageGRID. Ajoutez ces étapes avant de finaliser et d'utiliser le PlayBook.

RHEL

Pour RHEL, 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`

Ubuntu ou Debian

Pour Ubuntu ou Debian, les tâches d'installation fournies `storagegrid` exemple de rôle utiliser le `ansible.builtin.apt` module pour effectuer l'installation à partir des fichiers DEB locaux ou d'un référentiel apt 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 `ansible.builtin.apt` module:

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

Automatiser la configuration de StorageGRID

Une fois les nœuds grid déployés, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

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

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

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



Stockez le mot de passe de gestion et la phrase secrète de provisionnement à partir de la section des mots de passe du fichier modifié. `configure-storagegrid.json` fichier de configuration dans un emplacement sécurisé. Ces mots de passe sont requis pour les procédures d'installation, d'extension et de maintenance. Vous devez également sauvegarder les fichiers modifiés. `configure-storagegrid.json` fichier de configuration et stockez-le dans un endroit sûr.

Description de la tâche

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



Vous pouvez également configurer le système à l'aide de Grid Manager ou de l'API d'installation.

Étapes

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

Par exemple :

```
cd StorageGRID-Webscale-version/platform
```

où `platform` est `debs`, `rpms` ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

Par exemple :

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Résultat

Un fichier de module de récupération .zip est généré pendant le processus de configuration et est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.



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

Si vous avez indiqué que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` fichier et 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.
```

Automatisez le déploiement des nœuds de grille dans StorageGRID avec VMware vSphere

Vous pouvez utiliser l'outil VMware OVF pour automatiser le déploiement des nœuds grid. Vous pouvez également automatiser la configuration de StorageGRID.

Automatisez le déploiement de nœuds grid

Utilisez l'outil VMware OVF pour automatiser le déploiement des nœuds grid.

Avant de commencer

- Vous avez accès à un système Linux/Unix avec Bash 3.2 ou version ultérieure.
- Vous avez VMware vSphere avec vCenter
- Vous avez installé et correctement configuré VMware OVF Tool.
- Vous connaissez le nom d'utilisateur et le mot de passe permettant d'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 connecter aux machines virtuelles. Voir la `ovftool` documentation pour plus de détails.
- Vous connaissez l'URL d'infrastructure virtuelle (VI) pour l'emplacement dans vSphere où vous souhaitez déployer les machines virtuelles StorageGRID. Cette URL est généralement une vApp ou un pool de ressources. Par exemple : `vi://vcenter.example.com/vi/sgws`



Vous pouvez utiliser l'utilitaire VMware `ovftool` pour déterminer cette valeur (voir la [ovftool documentation](#) pour plus de détails).



Si vous déployez une vApp, les machines virtuelles ne démarrent pas automatiquement la première fois et vous devez les mettre sous tension manuellement.

- Vous avez recueilli toutes les informations requises pour le fichier de configuration du déploiement. Voir ["Collecte d'informations sur votre environnement de déploiement"](#) pour plus d'informations.
- Vous avez accès aux fichiers suivants à partir de l'archive d'installation de VMware pour StorageGRID :

Nom du fichier	Description
NetApp-SG-version-SHA.vmdk	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille. Remarque : ce fichier doit se trouver dans le même dossier que les <code>.ovf</code> fichiers et <code>.mf</code> .
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Le fichier modèle Open Virtualization format (<code>.ovf</code>) et le fichier manifeste (<code>.mf</code>) pour le déploiement du nœud d'administration principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Le fichier modèle (<code>.ovf</code>) et le fichier manifeste (<code>.mf</code>) pour le déploiement de nœuds Admin non primaires.
vsphere-gateway.ovf vsphere-gateway.mf	Le fichier modèle (<code>.ovf</code>) et le fichier manifeste (<code>.mf</code>) pour le déploiement des nœuds de passerelle.
vsphere-storage.ovf vsphere-storage.mf	Le fichier modèle (<code>.ovf</code>) et le fichier manifeste (<code>.mf</code>) pour le déploiement des nœuds de stockage basés sur des machines virtuelles.
deploy-vsphere-ovftool.sh	Le script de shell Bash utilisé pour automatiser le déploiement des nœuds de grille virtuels.
deploy-vsphere-ovftool-sample.ini	Exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> script.

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 utilisé par le `deploy-vsphere-ovftool.sh` script Bash. Vous pouvez modifier un exemple de fichier de configuration pour ne pas avoir à créer le fichier à partir de zéro.

Étapes

1. Faites une copie du fichier de configuration exemple (`deploy-vsphere-ovftool.sample.ini`). Enregistrez le nouveau fichier comme `deploy-vsphere-ovftool.ini` dans le même répertoire que

```
deploy-vmware-ovftool.sh.
```

2. Ouvrir `deploy-vmware-ovftool.ini`.
3. Entrez toutes les informations requises pour déployer des nœuds VMware Virtual Grid.

Voir [Paramètres du fichier de configuration](#) pour plus d'informations.

4. Une fois que vous avez saisi et vérifié toutes les informations nécessaires, enregistrez et fermez le fichier.

Paramètres du fichier de configuration

Le `deploy-vmware-ovftool.ini` fichier de configuration contient les paramètres requis pour déployer les nœuds de grille virtuelle.

Le fichier de configuration répertorie d'abord les paramètres globaux, puis répertorie les paramètres spécifiques au nœud dans les sections définies par nom de nœud. Lorsque le fichier est utilisé :

- *Paramètres globaux* sont appliqués à tous les nœuds de la grille.
- *Node-Specific parameters* remplace les paramètres globaux.

Paramètres globaux

Les paramètres globaux sont appliqués à tous les nœuds de la grille, sauf s'ils sont remplacés par des paramètres dans des sections individuelles. Placez les paramètres qui s'appliquent à plusieurs nœuds dans la section des paramètres globaux, puis remplacez ces paramètres si nécessaire dans les sections de nœuds individuels.

- **OVFTOOL_ARGUMENTS** : vous pouvez spécifier `OVFTOOL_ARGUMENTS` comme paramètres globaux, ou vous pouvez appliquer des arguments individuellement à des nœuds spécifiques. Par exemple :

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

Vous pouvez utiliser les `--powerOffTarget` options et `--overwrite` pour arrêter et remplacer des machines virtuelles existantes.



Vous devez déployer des nœuds dans différents datastores et spécifier `OVFTOOL_ARGUMENTS` pour chaque nœud, au lieu de global.

- **SOURCE** : chemin d'accès au (.vmdk`fichier modèle de machine virtuelle StorageGRID ) et aux `.ovf fichiers et .mf pour les nœuds de grille individuels. Par défaut, le répertoire courant est sélectionné.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET** : URL de l'infrastructure virtuelle VMware vSphere (vi) pour l'emplacement où StorageGRID sera déployé. Par exemple :

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, STATIQUES ou DHCP. La valeur par défaut est STATIQUE. Si tous les nœuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau Grid. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK** : masque de réseau pour le réseau de grille. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY** : passerelle réseau pour le réseau Grid. Si tous les nœuds ou la plupart utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU** : FACULTATIF. L'unité de transmission maximale (MTU) sur le réseau Grid. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Par exemple :

```
GRID_NETWORK_MTU = 9000
```

Si omis, 1400 est utilisé.

Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.



La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur virtuel dans vSphere auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.



Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau.

- **ADMIN_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, DÉSACTIVÉES, STATIQUE ou DHCP. La valeur par défaut EST DÉSACTIVÉE. Si tous les nœuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau Admin. Ce paramètre est requis, sauf si le réseau d'administration est désactivé. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Contrairement au réseau Grid Network, tous les nœuds n'ont pas besoin d'être connectés au même réseau Admin. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK** : le masque réseau du réseau Admin. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY** : passerelle réseau pour le réseau Admin. Ce paramètre est requis si vous utilisez l'adressage IP statique et que vous spécifiez des sous-réseaux externes dans LE paramètre ADMIN_NETWORK_ESL. (C'est-à-dire, ce n'est pas nécessaire si ADMIN_NETWORK_ESL est vide.) Si tous les nœuds ou la plupart utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL** : liste de sous-réseaux externes (routes) pour le réseau Admin, spécifiée comme liste de destinations de routage CIDR séparées par des virgules. Si tous les nœuds ou la plupart utilisent la même liste de sous-réseaux externes, vous pouvez la spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :


```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU** : FACULTATIF. Unité de transmission maximale (MTU) sur le réseau Admin. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. Si tous les nœuds ou la plupart utilisent le même MTU pour le réseau d'administration, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, DÉSACTIVÉES, STATIQUE ou DHCP. La valeur par défaut EST DÉSACTIVÉE. Si tous les nœuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau client. Ce paramètre est requis, sauf si le réseau client est désactivé. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Contrairement au réseau de grille, tous les nœuds n'ont pas besoin d'être connectés au même réseau client. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK** : le masque réseau du réseau client. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY** : passerelle réseau pour le réseau client. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU** : FACULTATIF. Unité de transmission maximale (MTU) sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise

entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. Si tous les nœuds ou la plupart utilisent le même MTU pour le réseau client, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAPPAGE** : remappe tout port utilisé par un nœud pour les communications internes de nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les stratégies de mise en réseau d'entreprise limitent un ou plusieurs ports utilisés par StorageGRID. Pour obtenir la liste des ports utilisés par StorageGRID, reportez-vous à la section communications internes des nœuds de grille et communications externes de la section "[Instructions de mise en réseau](#)".



Ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les terminaux de l'équilibreur de charge.



Si le PARAMÈTRE PORT_REMAPPAGE est défini uniquement, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes.

Le format utilisé est : *network type/protocol/default port used by grid node/new port*, où le type de réseau est grid, admin ou client et où le protocole est tcp ou udp.

Par exemple :

```
PORT_REMAP = client/tcp/18082/443
```

Utilisé seul, cet exemple de paramètre mappe de façon symétrique les communications entrantes et sortantes du nœud de grille entre le port 18082 et le port 443. Si utilisé conjointement avec PORT_REMAPPAGE_INBOUND, cet exemple de paramètre mappe les communications sortantes du port 18082 au port 443.

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_REMAPPAGE_INBOUND** : remappe les communications entrantes pour le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais que vous ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées.



Ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les terminaux de l'équilibreur de charge.

Le format utilisé est : *network type/protocol/_default port used by grid node/new port*,

où le type de réseau est grid, admin ou client et où le protocole est tcp ou udp.

Par exemple :

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Dans cet exemple, le trafic envoyé au port 443 passe par un pare-feu interne et le dirige vers le port 18082, où le nœud de la grille écoute les requêtes S3.

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
```

- **TEMPORAIRE_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 de StorageGRID, ou à l'aide de SSH, avant que le nœud ne rejoigne la grille.



Si la totalité ou la plupart des nœuds utilisent le même type de mot de passe d'installation temporaire, spécifiez le type dans la section paramètre global. Ensuite, vous pouvez utiliser un paramètre différent pour un nœud individuel. Par exemple, si vous sélectionnez **utiliser le mot de passe personnalisé** globalement, vous pouvez utiliser **CUSTOM_TEMPORAIRES_PASSWORD=<password>** pour définir le mot de passe de chaque nœud.

TEMPORAIRE_PASSWORD_TYPE peut être l'un des éléments suivants :

- **Utiliser le nom de nœud** : le nom de nœud est utilisé comme mot de passe d'installation temporaire et permet d'accéder 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, reportez-vous à la section "[Résoudre les problèmes d'installation](#)".
- **Utiliser mot de passe personnalisé** : la valeur fournie avec **CUSTOM_TEMPORAIRES_PASSWORD=<password>** est utilisée comme mot de passe d'installation temporaire et permet d'accéder à la console VM, à l'API d'installation StorageGRID et à SSH.



Vous pouvez également omettre le paramètre **TEMPORAIRE_PASSWORD_TYPE** et spécifier uniquement **PERSONNALISÉ_TEMPORAIRE_PASSWORD=<password>**.

- **CUSTOM_TEMPORAIRES_PASSWORD=<password>** Facultatif. Mot de passe temporaire à utiliser lors de l'installation lors de l'accès à la console de la machine virtuelle, à l'API d'installation StorageGRID et à SSH. Ignoré si **TEMPORAIRE_PASSWORD_TYPE** est défini sur **utiliser le nom de 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 Grid Manager. Vous pouvez remplacer cette valeur en spécifiant le paramètre optionnel `NOM_NOEUD` pour le noeud.
- **NODE_TYPE** : `VM_Admin_Node`, `VM_Storage_Node` ou `VM_API_Gateway_Node`
- **STORAGE_TYPE** : combiné, données ou métadonnées. Si ce paramètre facultatif n'est pas spécifié, il devient par défaut combiné (données et métadonnées) pour les nœuds de stockage. Pour plus d'informations, voir "[Types de nœuds de stockage](#)".
- **GRID_NETWORK_IP** : adresse IP du nœud sur le réseau Grid.
- **ADMIN_NETWORK_IP** : adresse IP du noeud sur le réseau Admin. Obligatoire uniquement si le nœud est connecté au réseau Admin et QUE `ADMIN_NETWORK_CONFIG` est défini SUR STATIQUE.
- **CLIENT_NETWORK_IP** : adresse IP du noeud sur le réseau client. Requis uniquement si le nœud est connecté au réseau client et QUE `CLIENT_NETWORK_CONFIG` pour ce nœud est défini sur STATIQUE.
- **ADMIN_IP** : adresse IP du nœud d'administration principal sur le réseau Grid. Utilisez la valeur que vous spécifiez comme `GRID_NETWORK_IP` pour le noeud d'administration principal. Si vous omettez ce paramètre, le nœud tente de détecter l'IP du nœud d'administration principal à l'aide de mDNS. Pour plus d'informations, voir "[Mode de détection des nœuds du grid sur le nœud d'administration principal](#)".



Le paramètre `ADMIN_IP` est ignoré pour le nœud d'administration principal.

- Tous les paramètres qui n'ont pas été définis globalement. Par exemple, si un nœud est associé au réseau Admin et que vous n'avez pas spécifié les paramètres `ADMIN_NETWORK` globalement, vous devez les spécifier pour le nœud.

Nœud d'administration principal

Les paramètres supplémentaires suivants sont requis pour le nœud d'administration principal :

- **NODE_TYPE** : `VM_Admin_Node`
- **ADMIN_ROLE** : principal

Cet exemple d'entrée concerne un noeud d'administration principal sur les trois réseaux :

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node
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 sont affectés à deux disques durs supplémentaires de 200 Go pour l'audit et l'utilisation de la base de données. Vous pouvez augmenter ces paramètres à l'aide du paramètre `DISQUE`. Par exemple :

```
DISK = INSTANCES=2, CAPACITY=300
```



Pour les nœuds Admin, LES INSTANCES doivent toujours être égales à 2.

Nœud de stockage

Le paramètre supplémentaire suivant est requis pour les nœuds de stockage :

- **NODE_TYPE** : VM_Storage_Node

Cet exemple d'entrée concerne un nœud de stockage qui se trouve sur la grille et les réseaux d'administration, mais pas sur le réseau client. Ce nœud utilise le paramètre ADMIN_IP pour spécifier l'adresse IP du nœud d'administration principal sur le réseau Grid.

```
[DC1-S1]
NODE_TYPE = VM_Storage_Node

GRID_NETWORK_IP = 10.1.0.3
ADMIN_NETWORK_IP = 10.3.0.3

ADMIN_IP = 10.1.0.2
```

Ce deuxième exemple d'entrée concerne un nœud de stockage sur un réseau client dans lequel la stratégie de réseau d'entreprise du client indique qu'une application client S3 n'est autorisée qu'à accéder au nœud de stockage via le port 80 ou 443. Cet exemple de fichier de configuration utilise PORT_REMAP pour permettre au nœud de stockage d'envoyer et de recevoir des messages S3 sur le port 443.

```
[DC2-S1]
NODE_TYPE = VM_Storage_Node

GRID_NETWORK_IP = 10.1.1.3
CLIENT_NETWORK_IP = 10.4.1.3
PORT_REMAP = client/tcp/18082/443

ADMIN_IP = 10.1.0.2
```

Le dernier exemple crée un remappage symétrique pour le trafic ssh du port 22 au port 3022, mais définit explicitement les valeurs pour le trafic entrant et sortant.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

Les paramètres supplémentaires suivants sont facultatifs pour les nœuds de stockage :

- **DISQUE** : par défaut, les nœuds de stockage sont affectés à trois disques de 4 To pour une utilisation RangeDB. Vous pouvez augmenter ces paramètres à l'aide du paramètre DISQUE. Par exemple :

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE** : par défaut, tous les nouveaux nœuds de stockage sont configurés pour stocker à la fois les données d'objet et les métadonnées, appelées *Combined Storage Node*. 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 du réseau client n'a été spécifié dans la section globale du fichier de configuration. Il faut donc les spécifier pour le nœud :

```
[DC1-G1]
NODE_TYPE = VM_API_Gateway

GRID_NETWORK_IP = 10.1.0.5
ADMIN_NETWORK_IP = 10.3.0.5

CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_TARGET = SG Client Network
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.4.0.1
CLIENT_NETWORK_IP = 10.4.0.5

ADMIN_IP = 10.1.0.2
```

Nœud d'administration non primaire

Les paramètres supplémentaires suivants sont requis pour les nœuds d'administration non primaires :

- **NODE_TYPE** : VM_Admin_Node
- **ADMIN_ROLE** : non-Primary

Cet exemple d'entrée concerne un nœud d'administration non primaire qui n'est pas sur le réseau client :

```
[DC2-ADM1]
ADMIN_ROLE = Non-Primary
NODE_TYPE = VM_Admin_Node

GRID_NETWORK_TARGET = SG Grid Network
GRID_NETWORK_IP = 10.1.0.6
ADMIN_NETWORK_IP = 10.3.0.6

ADMIN_IP = 10.1.0.2
```

Le paramètre supplémentaire suivant est facultatif pour les nœuds d'administration non primaires :

- **DISQUE** : par défaut, les nœuds d'administration sont affectés à deux disques durs supplémentaires de 200 Go pour l'audit et l'utilisation de la base de données. Vous pouvez augmenter ces paramètres à l'aide du paramètre DISQUE. Par exemple :

```
DISK = INSTANCES=2, CAPACITY=300
```



Pour les nœuds Admin, LES INSTANCES doivent toujours être égales à 2.

Exécutez le script Bash

Vous pouvez utiliser `deploy-vsphere-ovftool.sh` le script Bash et le fichier de configuration `deploy-vsphere-ovftool.ini` que vous avez modifié pour automatiser le déploiement des nœuds StorageGRID dans VMware vSphere.

Avant de commencer

Vous avez créé un fichier de configuration `deploy-vsphere-ovftool.ini` pour votre environnement.

Vous pouvez utiliser l'aide disponible avec le script Bash en entrant les commandes d'aide (`-h/--help`). Par exemple :

```
./deploy-vsphere-ovftool.sh -h
```

ou

```
./deploy-vsphere-ovftool.sh --help
```

Étapes

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

Par exemple :

```
cd StorageGRID-Webscale-version/vsphere
```

3. Pour déployer tous les nœuds de la grille, exécutez le script Bash avec les options appropriées pour votre environnement.

Par exemple :

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-vsphere-ovftool.ini
```

4. Si un nœud de grille n'a pas pu être déployé en raison d'une erreur, résolvez l'erreur et relancez le script de Bash pour ce nœud uniquement.

Par exemple :

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single -node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

Le déploiement est terminé lorsque l'état de chaque nœud est « passé ».

Deployment Summary

node	attempts	status
DC1-ADM1	1	Passed
DC1-G1	1	Passed
DC1-S1	1	Passed
DC1-S2	1	Passed
DC1-S3	1	Passed

Automatiser la configuration de StorageGRID

Une fois les nœuds grid déployés, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

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

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

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



Stockez le mot de passe de gestion et la phrase secrète de provisionnement à partir de la section des mots de passe du fichier modifié. `configure-storagegrid.json` fichier de configuration dans un emplacement sécurisé. Ces mots de passe sont requis pour les procédures d'installation, d'extension et de maintenance. Vous devez également sauvegarder les fichiers modifiés. `configure-storagegrid.json` fichier de configuration et stockez-le dans un endroit sûr.

Description de la tâche

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



Vous pouvez également configurer le système à l'aide de Grid Manager ou de l'API d'installation.

Étapes

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

Par exemple :

```
cd StorageGRID-Webscale-version/platform
```

où `platform` est `debs`, `rpms` ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

Par exemple :

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Résultat

Un fichier de module de récupération `.zip` est généré pendant le processus de configuration et est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.



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

Si vous avez indiqué que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` fichier et 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 associées

- ["Accédez au Grid Manager"](#)
- ["Installation de l'API REST"](#)

Déployer des nœuds de grille virtuels

Collectez des informations sur votre environnement VMware pour StorageGRID

Avant de déployer les nœuds de la grille, vous devez collecter des informations sur la configuration de votre réseau et l'environnement VMware.



Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

Informations sur VMware

Vous devez accéder à l'environnement de déploiement et collecter des informations sur l'environnement VMware, les réseaux créés pour les réseaux Grid, Admin et client, ainsi que les types de volume de stockage que vous envisagez d'utiliser pour les nœuds de stockage.

Vous devez collecter des informations sur votre environnement VMware, notamment :

- Nom d'utilisateur et mot de passe d'un compte VMware vSphere disposant des autorisations appropriées pour terminer le déploiement.
- Informations sur l'hôte, le datastore et la configuration réseau pour chaque machine virtuelle de nœud StorageGRID.



VMware Live vMotion provoque l'augmentation de l'horloge de la machine virtuelle et n'est pas pris en charge pour les nœuds grid d'aucun type. Bien que les temps d'horloge rares et incorrects peuvent entraîner une perte de données ou des mises à jour de la configuration.

Informations sur le réseau

Vous devez collecter des informations sur le réseau VMware créé pour le réseau StorageGRID Grid Network (obligatoire), notamment :

- Nom du réseau.
- Méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
 - Si vous utilisez des adresses IP statiques, les informations de mise en réseau requises pour chaque nœud de la grille (adresse IP, passerelle, masque de réseau).
 - Si vous utilisez DHCP, l'adresse IP du nœud d'administration principal sur le réseau Grid. Voir "[Mode de détection des nœuds du grid sur 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 :

- Nom du réseau.
- Méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
 - Si vous utilisez des adresses IP statiques, les informations de mise en réseau requises pour chaque nœud de la grille (adresse IP, passerelle, masque de réseau).
 - Si vous utilisez DHCP, l'adresse IP du nœud d'administration principal sur le réseau Grid. Voir "[Mode de détection des nœuds du grid sur le nœud d'administration principal](#)" pour plus d'informations.

- La liste des sous-réseaux externes (ESL) pour le réseau Admin.

Informations sur le réseau client

Pour les nœuds qui seront connectés au réseau client StorageGRID en option, vous devez collecter des informations sur le réseau VMware créé pour ce réseau, notamment :

- Nom du réseau.
- Méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
- Si vous utilisez des adresses IP statiques, les informations de mise en réseau requises pour chaque nœud de la grille (adresse IP, passerelle, masque de réseau).

Informations sur les interfaces supplémentaires

Vous pouvez éventuellement ajouter une jonction ou des interfaces d'accès à la machine virtuelle dans vCenter après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un nœud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page HA Groups de la grille Manager.

- Si vous ajoutez une interface de jonction, configurez une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent. Voir ["Configurez les interfaces VLAN"](#).
- Si vous ajoutez une interface d'accès, vous devez l'ajouter directement aux groupes haute disponibilité. Voir ["configurez les groupes haute disponibilité"](#).

Volumes de stockage pour les nœuds de stockage virtuels

Vous devez collecter les informations suivantes pour les nœuds de stockage basés sur des machines virtuelles :

- Le nombre et la taille des volumes de stockage (LUN de stockage) que vous prévoyez d'ajouter. Voir ["Les besoins en matière de stockage et de performances"](#).

Informations de configuration de la grille

Vous devez collecter des informations pour configurer votre grille :

- Licence Grid
- Adresses IP du serveur NTP (Network Time Protocol)
- Adresses IP du serveur DNS

Créer des fichiers de configuration de nœud StorageGRID pour les déploiements Linux

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



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Emplacement des fichiers de configuration de nœud

Placez le fichier de configuration de chaque nœud StorageGRID dans le `/etc/storagegrid/nodes` répertoire de l'hôte sur lequel le nœud sera exécuté. Par exemple, si vous prévoyez d'exécuter un nœud d'administration, un nœud de passerelle et un nœud de stockage sur HostA, vous devez placer trois fichiers de configuration de nœud dans `/etc/storagegrid/nodes` sur HostA.

Vous pouvez créer les fichiers de configuration directement sur chaque hôte à l'aide d'un éditeur de texte, tel que vim ou nano, ou les créer ailleurs et les déplacer vers chaque hôte.

Dénomination des fichiers de configuration des nœuds

Les noms des fichiers de configuration sont importants. Le format est `node-name.conf`, où `node-name` est un nom que vous attribuez au nœud. Ce nom apparaît dans le programme d'installation StorageGRID et sert aux opérations de maintenance de nœud, telles que la migration de nœud.

Les noms de nœud doivent respecter les règles suivantes :

- Doit être unique
- Doit commencer par une lettre
- Peut contenir les caractères A à Z et a à z
- Peut contenir les chiffres 0 à 9
- Peut contenir un ou plusieurs traits d'Union (-)
- Ne doit pas comporter plus de 32 caractères, sans compter le `.conf` poste

Les fichiers `/etc/storagegrid/nodes` qui ne respectent pas ces conventions de dénomination ne seront pas analysés par le service hôte.

Si une topologie multisite est planifiée pour votre grille, il se peut qu'un schéma de nommage de nœud type soit :

```
site-nodetype-nodenumbers.conf
```

Par exemple, vous pouvez utiliser `dc1-adm1.conf` pour le premier nœud d'administration du data Center 1 et `dc2-sn3.conf` pour le troisième nœud de stockage du data Center 2. Toutefois, vous pouvez utiliser n'importe quel schéma, à condition que tous les noms de nœud suivent les règles d'attribution de nom.

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 les règles suivantes :

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

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

- **Obligatoire** : requis pour chaque nœud ou pour les types de nœuds spécifiés
- **Meilleure pratique** : facultative, bien que recommandée
- **Facultatif** : facultatif pour tous les nœuds

Admin clés réseau

IP_ADMIN

Valeur	Désignation
Adresse IPv4 du réseau de grille du nœud d'administration que vous souhaitez utiliser pour installer le nœud basé sur Linux. Pour la récupération, utilisez l'adresse IP du nœud d'administration principal si disponible ; sinon, utilisez l'adresse IP d'un nœud d'administration non principal. Si vous omettez ce paramètre, le nœud tente de découvrir un nœud d'administration principal à l'aide de mDNS. "Mode de détection des nœuds du grid sur le nœud d'administration principal"	Et des meilleures pratiques

CONFIG RÉSEAU_ADMIN

Valeur	Désignation
DHCP, STATIQUE OU DÉSACTIVÉ	Facultatif

ADMIN_NETWORK_ESL

Valeur	Désignation
Liste de sous-réseaux séparés par des virgules en notation CIDR à laquelle ce nœud doit communiquer à l'aide de la passerelle Admin Network. Exemple : 172.16.0.0/21,172.17.0.0/21	Facultatif

PASSERELLE RÉSEAU_ADMIN

Valeur	Désignation
Adresse IPv4 de la passerelle réseau d'administration locale pour ce nœud. Doit être sur le sous-réseau défini par ADMIN_NETWORK_IP et ADMIN_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP. Exemples : 1.1.1.1 10.224.4.81	Obligatoire si ADMIN_NETWORK_ESL est spécifié. Facultatif autrement.

IP RÉSEAU_ADMIN

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

ADMIN_NETWORK_MAC

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

ADMIN_NETWORK_MASK

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

MTU_RÉSEAU_ADMIN

Valeur	Désignation
Unité de transmission maximale (MTU) pour ce nœud sur le réseau Admin. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire. Exemples : 1500 8192	Facultatif

CIBLE_RÉSEAU_ADMIN

Valeur	Désignation
Nom de l'unité hôte que vous utiliserez pour accéder au réseau d'administration par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth). Meilleure pratique: spécifiez une valeur même si ce nœud ne possède pas d'adresse IP de réseau Admin initialement. Vous pouvez ensuite ajouter une adresse IP de réseau d'administration plus tard, sans avoir à reconfigurer le nœud sur l'hôte. Exemples : bond0.1002 ens256	Et des meilleures pratiques

TYPE_CIBLE RÉSEAU_ADMIN

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

ADMIN_NETWORK_TARGET_TYPE_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 hôte cible sur le réseau d'administration. Pour plus de détails sur le clonage MAC pour Linux, voir "Considérations et recommandations relatives au clonage d'adresses MAC".	Et des meilleures pratiques

RÔLE_ADMINISTRATEUR

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.	Requis lorsque NODE_TYPE = VM_Admin_Node Facultatif autrement.

Bloquer les clés de périphérique

JOURNAUX_AUDIT_BLOC_PÉRIPHÉRIQUE

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

BLOCK_DEVICE_RANGEDB_NNN

Valeur	Désignation
Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour le stockage objet permanent. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Storage_noeud ; ne la spécifiez pas pour d'autres types de nœuds. Seul LE BLOCK_DEVICE_RANGEDB_000 est requis ; le reste est facultatif. Le dispositif de bloc spécifié pour BLOCK_DEVICE_RANGEDB_000 doit être d'au moins 4 To ; les autres peuvent être plus petits. Ne laissez pas d'espace. Si vous spécifiez BLOCK_DEVICE_RANGEDB_005, vous devez également spécifier BLOCK_DEVICE_RANGEDB_004. Remarque : pour la compatibilité avec les déploiements existants, les clés à deux chiffres sont prises en charge pour les nœuds mis à niveau. Exemples : <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-rangedb-000</pre>	Obligatoire : 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

BLOQUER_LES_TABLES_PÉRIPHÉRIQUES

Valeur	Désignation
Chemin et nom du fichier spécial de l'unité de bloc ce noeud sera utilisé pour le stockage persistant des tables de base de données. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Admin_noeud ; ne la spécifiez pas pour d'autres types de noeuds. Exemples : <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

BLOCK_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 réseau du 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 CLIENT_NETWORK_IP et CLIENT_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP. Exemples : 1.1.1.1 10.224.4.81	Facultatif

IP_RÉSEAU_CLIENT

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau client. Cette clé n'est requise que lorsque CLIENT_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs. Exemples : 1.1.1.1 10.224.4.81	Requis lorsque CLIENT_NETWORK_CONFIG = STATIQUE Facultatif autrement.

CLIENT_RÉSEAU_MAC

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

MASQUE_RÉSEAU_CLIENT

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

MTU_CLIENT RÉSEAU

Valeur	Désignation
Unité de transmission maximale (MTU) pour ce nœud sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire. Exemples : 1500 8192	Facultatif

CIBLE RÉSEAU CLIENT

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour accéder au réseau client par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET. Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth). Meilleure pratique : Indiquez une valeur même si ce nœud ne possède pas d'adresse IP de réseau client au départ. Vous pouvez ensuite ajouter une adresse IP du réseau client ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte. Exemples : bond0.1003 ens423	Et des meilleures pratiques

TYPE_CIBLE RÉSEAU_CLIENT

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

CLIENT RÉSEAU_CIBLE_TYPE_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 hôte sur le réseau client. Pour plus de détails sur le clonage MAC pour Linux, voir "Considérations et recommandations relatives au clonage d'adresses MAC".	Et des meilleures pratiques

Touches réseau de la grille

CONFIG RÉSEAU_GRID

Valeur	Désignation
STATIQUE ou DHCP La valeur par défaut est STATIQUE si elle n'est pas spécifiée.	Et des meilleures pratiques

PASSERELLE_RÉSEAU_GRILLE

Valeur	Désignation
Adresse IPv4 de la passerelle réseau Grid locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par GRID_NETWORK_IP et GRID_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP. Si le réseau Grid est un sous-réseau unique sans passerelle, utilisez soit l'adresse de passerelle standard pour le sous-réseau (X. Y.1), soit la valeur DE GRID_NETWORK_IP de ce nœud. Ces valeurs simplifient les extensions potentielles du réseau Grid.	Obligatoire

IP_RÉSEAU_GRID

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

GRID_RÉSEAU_MAC

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

GRID_NETWORK_MASK

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

GRID_NETWORK_MTU

Valeur	Désignation
Unité de transmission maximale (MTU) pour ce nœud sur le réseau Grid. Ne spécifiez pas si GRID_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire. IMPORTANT : pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte Grid Network MTU mismatch est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Exemples : 1500 8192	Facultatif

CIBLE_RÉSEAU_GRILLE

Valeur	Désignation
Nom de l'unité hôte que vous utiliserez pour accéder au réseau Grid par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth). Exemples : bond0.1001 ens192	Obligatoire

TYPE_CIBLE RÉSEAU GRILLE

Valeur	Désignation
DedicatedInterface (Il s'agit de 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 de la grille. Pour plus de détails sur le clonage MAC pour Linux, voir "Considérations et recommandations relatives au clonage d'adresses MAC"	Et des meilleures pratiques

Clé de mot de passe d'installation (temporaire)

HACHAGE_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 lors de l'installation. Remarque : définissez un mot de passe d'installation sur le nœud Admin 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 lorsque l'installation est 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 de StorageGRID. Doit être un <code>crypt()</code> hachage de mot de passe SHA-512 au format <code>\$6\$<salt>\$<password hash></code> pour un mot de passe d'au moins 8 et pas plus de 32 caractères. Ce hachage peut être généré à l'aide d'outils de l'interface de ligne de commande, tels que la <code>openssl passwd</code> commande en mode SHA-512.	Et des meilleures pratiques

Clé d'interface

INTERFACE_TARGET_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 des interfaces VLAN et sur la page des groupes haute disponibilité. 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 l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.	Facultatif

Clé RAM maximale

RAM_MAXIMALE

Valeur	Désignation
Quantité maximale de RAM que ce nœud est autorisé à consommer. Si cette clé est omise, le nœud n'a aucune restriction de mémoire. Lorsque vous définissez ce champ pour un nœud de niveau production, indiquez une valeur inférieure d'au moins 24 Go et de 16 à 32 Go à la mémoire RAM totale du système. Remarque : la valeur de la RAM affecte l'espace réservé des métadonnées réelles d'un nœud. Voir la "Description de l'espace réservé aux métadonnées". Le format de ce champ est <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_NŒUD

Valeur	Désignation
Type de nœud : • Nœud_admin_VM • Nœud_stockage_VM • VM_Archive_Node • Passerelle_API_VM	Obligatoire

STORAGE_TYPE

Valeur	Désignation
Définit le type d'objets qu'un nœud de stockage contient. Pour plus d'informations, voir "Types de nœuds de stockage". Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Storage_noeud ; ne la spécifiez pas pour d'autres types de noeuds. Types de stockage : • combinés • les données • les métadonnées Remarque : si le TYPE_STOCKAGE n'est pas spécifié, le type de noeud de stockage est défini sur combiné (données et métadonnées) par défaut.	Facultatif

Touches de remap de port



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à "[Supprimez les mappes de ports sur les hôtes bare Metal](#)".

SCHÉMA DE PORT

Valeur	Désignation
Permet de remapper tout port utilisé par un nœud pour les communications internes de nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les stratégies de mise en réseau d'entreprise limitent un ou plusieurs ports utilisés par StorageGRID, comme décrit dans "Communications internes sur les nœuds de la grille" ou "Communications externes". IMPORTANT : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les noeuds finaux de l'équilibreur de charge. Remarque : si seul PORT_REMAPPAGE est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes. Le format utilisé est : <i>network type/protocol/default port used by grid node/new port</i>, où <i>network type</i> est <i>grid</i>, <i>admin</i> ou <i>client</i>, et <i>tcp</i> ou <i>protocol udp</i>. 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_REMAPPAGE_ENTRANT

Valeur	Désignation
Mappe de nouveau les communications entrantes sur le port spécifié. Si vous spécifiez <code>PORT_REMAP_INBOUND</code> mais que vous ne spécifiez pas de valeur pour <code>PORT_REMAP</code>, les communications sortantes pour le port sont inchangées. IMPORTANT : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les nœuds finaux 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 <code>grid</code>, <code>admin</code> ou <code>client</code>, et <code>tcp</code> ou <code>protocol udp</code>. 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 la grille découvrent le nœud d'administration principal dans StorageGRID

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

Pour vous assurer qu'un nœud de grille peut accéder au nœud d'administration principal, vous pouvez effectuer l'une des opérations suivantes lors du déploiement du nœud :

- Vous pouvez utiliser le paramètre `ADMIN_IP` pour saisir manuellement l'adresse IP du nœud d'administration principal.
- Vous pouvez omettre le paramètre `ADMIN_IP` pour que le nœud de la grille détecte automatiquement la valeur. La détection automatique est particulièrement utile lorsque le réseau Grid utilise DHCP pour attribuer l'adresse IP au nœud d'administration principal.

La découverte automatique du nœud d'administration principal s'effectue à l'aide d'un système de noms de domaine multicast (mDNS). Lors du premier démarrage du nœud d'administration principal, il publie son adresse IP à l'aide de mDNS. Les autres nœuds du même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, comme le trafic IP multicast n'est généralement pas routable entre les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud Admin principal.

Si vous utilisez la détection automatique :



- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publie ensuite l'adresse IP du nœud d'administration principal pour les autres nœuds du sous-réseau à détecter avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le trafic IP multicast dans un sous-réseau.

Déployez des nœuds de grille en tant que machines virtuelles pour StorageGRID avec VMware vSphere

Vous utilisez le client Web VMware vSphere pour déployer chaque nœud de grid en tant que machine virtuelle. Pendant le déploiement, chaque nœud de grid est créé et connecté à un ou plusieurs réseaux StorageGRID.

Si vous avez besoin de déployer des nœuds de stockage de l'appliance StorageGRID, consultez la section ["Déployez le nœud de stockage de l'appliance"](#).

Vous pouvez également remapper les ports du nœud ou augmenter les paramètres de processeur ou de mémoire du nœud avant de le mettre sous tension.

Avant de commencer

- Vous avez examiné ["planification et préparation de l'installation"](#) la procédure à suivre et vous avez compris les exigences en matière de logiciels, de CPU et de RAM, de stockage et de performances.
- Vous connaissez déjà l'hyperviseur VMware vSphere et êtes déjà familiarisé avec le déploiement de serveurs virtuels dans cet environnement.



Ce open-vm-tools package, une implémentation open source similaire aux outils VMware, est inclus dans la machine virtuelle StorageGRID. Vous n'avez pas besoin d'installer VMware Tools manuellement.

- Vous avez téléchargé et extrait la version correcte de l'archive d'installation StorageGRID pour VMware.



Si vous déployez le nouveau nœud dans le cadre d'une opération d'extension ou de restauration, vous devez utiliser la version d'StorageGRID en cours d'exécution sur la grille.

- Vous disposez du (.vmdk`fichier StorageGRID Virtual machine Disk) :

```
NetApp-SG-version-SHA.vmdk
```

- Vous disposez des .ovf fichiers et .mf pour chaque type de nœud de grille que vous déployez :

Nom du fichier	Description
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Fichier modèle et fichier manifeste pour le nœud d'administration principal.

Nom du fichier	Description
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Fichier modèle et fichier manifeste pour un nœud d'administration non primaire.
vsphere-storage.ovf vsphere-storage.mf	Fichier modèle et fichier manifeste pour un nœud de stockage.
vsphere-gateway.ovf vsphere-gateway.mf	Fichier modèle et fichier manifeste pour un nœud passerelle.

- Les `.vdmk` fichiers, `.ovf` et `.mf` se trouvent tous dans le même répertoire.
- Vous disposez d'un plan pour réduire les domaines d'échec. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un 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 entraînerait un problème de domaine de défaillance inacceptable.

- Si vous déployez un nœud dans le cadre d'une opération d'extension ou de restauration, vous disposez du ["Instructions d'extension d'un système StorageGRID"](#) ou du ["instructions de récupération et de maintenance"](#).
- Si vous déployez un nœud StorageGRID en tant que machine virtuelle avec un stockage affecté à un système NetApp ONTAP, vous avez confirmé que cette FabricPool règle n'est pas activée pour le volume. Par exemple, si un nœud StorageGRID s'exécute en tant que machine virtuelle sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n'est pas activée pour le volume qui sauvegarde le datastore du nœud. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Description de la tâche

Suivez ces instructions pour déployer au départ des nœuds VMware, ajouter un nouveau nœud VMware dans une extension ou remplacer un nœud VMware dans le cadre d'une opération de restauration. Sauf comme indiqué dans les étapes, la procédure de déploiement des nœuds est la même pour tous les types de nœuds, y compris les nœuds d'administration, les nœuds de stockage et les nœuds de passerelle.

Si vous installez un nouveau système StorageGRID :

- Vous pouvez déployer les nœuds dans l'ordre de votre choix.
- Vous devez vous assurer que chaque machine virtuelle peut se connecter au nœud d'administration principal via le réseau Grid.
- Vous devez déployer tous les nœuds de la grille avant de configurer la grille.

Si vous effectuez une opération d'extension ou de reprise :

- Vous devez vous assurer que la nouvelle machine virtuelle peut se connecter 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 du remap des ports n'est pas terminée.



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à ["Supprimez les mappes de ports sur les hôtes bare Metal"](#).

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. Fournissez un nom pour la machine virtuelle.

La pratique standard consiste à utiliser le même nom pour la machine virtuelle et le nœud de grille.

3. Placez la machine virtuelle dans le pool de ressources ou vApp approprié.
4. Si vous déployez le nœud d'administration principal, lisez et acceptez le contrat de licence de l'utilisateur final.

Selon votre version de vCenter, l'ordre des étapes varie en fonction de l'acceptation du contrat de licence de l'utilisateur final, en précisant le nom de la machine virtuelle et en sélectionnant un datastore.

5. Sélectionnez le stockage de la machine virtuelle.

Si vous déployez un nœud dans le cadre d'une opération de restauration, suivez les instructions de la section [étape de restauration du stockage](#) pour ajouter de nouveaux disques virtuels, rattacher des disques durs virtuels à partir du nœud de grille défaillant, ou les deux.

Lors du déploiement d'un nœud de stockage, utilisez au moins 3 volumes de stockage, chaque volume de stockage étant de 4 To ou plus. Vous devez affecter au moins 4 To au volume 0.



Le fichier .ovf de nœud de stockage définit plusieurs VMDK pour le stockage. À moins que ces VMDK ne répondent à vos besoins de stockage, vous devez les supprimer et attribuer des VMDK ou des RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus fréquemment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo).



Certaines installations StorageGRID peuvent utiliser des volumes de stockage plus grands et plus actifs que les charges de travail virtualisées standard. Vous devrez peut-être régler certains paramètres de l'hyperviseur, tels que `MaxAddressableSpaceTB`, pour obtenir des performances optimales. Si vous rencontrez des problèmes de performances médiocres, contactez votre support de virtualisation pour déterminer si votre environnement peut bénéficier du réglage de la configuration propre aux charges de travail.

6. Sélectionnez réseaux.

Déterminez les réseaux StorageGRID que le nœud utilisera en sélectionnant un réseau de destination pour chaque réseau source.

- Le réseau Grid est requis. Vous devez sélectionner un réseau de destination dans l'environnement vSphere. + le réseau de grille est utilisé pour tout le trafic StorageGRID interne. Elle assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux. Tous les nœuds du réseau Grid doivent pouvoir communiquer avec tous les autres nœuds.
- Si vous utilisez le réseau Admin, sélectionnez un autre réseau de destination dans l'environnement vSphere. Si vous n'utilisez pas le réseau d'administration, sélectionnez la même destination que celle que vous avez sélectionnée pour le réseau en grille.
- Si vous utilisez le réseau client, sélectionnez un autre réseau de destination dans l'environnement vSphere. Si vous n'utilisez pas le réseau client, sélectionnez la destination que vous avez sélectionnée pour le réseau Grid.
- Si vous utilisez un réseau Admin ou client, les nœuds ne doivent pas nécessairement se trouver sur les mêmes réseaux Admin 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 la grille, vous devez entrer 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 que vous puissiez accéder à la console VM 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 lors de l'installation du nœud. Une fois qu'un nœud a été ajouté à la grille, vous pouvez y accéder à l'aide du "[mot de passe de la console du nœud](#)", qui est répertorié dans `Passwords.txt` le fichier du progiciel de récupération.

- **Utiliser le nom de nœud** : la valeur que vous avez fournie pour le champ **Nom de nœud** est utilisée comme mot de passe d'installation temporaire.
- **Utiliser 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, reportez-vous à la section "[Résoudre les problèmes d'installation](#)".

c. Si vous avez sélectionné **utiliser mot de passe personnalisé**, indiquez le mot de passe d'installation temporaire que vous souhaitez utiliser dans le champ **Mot de passe personnalisé**.

d. Dans la section **Grid Network (eth0)**, sélectionnez STATIQUE ou DHCP pour la configuration **Grid network IP**.

- Si vous sélectionnez STATIQUE, saisissez l'adresse IP * réseau Grid*, **masque réseau Grid**, **passerelle réseau Grid** et **MTU réseau Grid**.
- Si vous sélectionnez DHCP, l'adresse IP * réseau Grid*, **masque de réseau Grid** et **passerelle réseau Grid** sont automatiquement affectées.

e. Dans le champ **IP d'administration principale**, entrez l'adresse IP du nœud d'administration principal pour le réseau de grille.

Si vous omettez l'adresse IP du nœud d'administration principal, l'adresse IP est automatiquement découverte si le nœud d'administration principal, ou au moins un autre nœud de la grille avec ADMIN_IP configuré, est présent sur le même sous-réseau. Cependant, il est recommandé de définir ici l'adresse IP du nœud d'administration principal.

f. Dans la section **Admin Network (eth1)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la configuration **Admin network IP**.

- Si vous ne souhaitez pas utiliser le réseau d'administration, sélectionnez DÉSACTIVÉ et entrez **0.0.0.0** pour l'adresse IP du réseau d'administration. Vous pouvez laisser les autres champs vides.
- Si vous sélectionnez STATIQUE, saisissez l'adresse IP* du réseau **Admin**, ***masque réseau Admin**, **passerelle réseau Admin** et **MTU du réseau Admin**.
- Si vous sélectionnez STATIQUE, entrez la liste **réseau d'administration externe de sous-réseau**. Vous devez également configurer une passerelle.
- Si vous sélectionnez DHCP, l'adresse IP **réseau Admin**, **masque réseau Admin** et **passerelle réseau Admin** sont automatiquement affectées.

g. Dans la section **réseau client (eth2)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la configuration **IP réseau client**.

- Si vous ne souhaitez pas utiliser le réseau client, sélectionnez DÉSACTIVÉ et entrez **0.0.0.0** pour l'adresse IP du réseau client. Vous pouvez laisser les autres champs vides.
- Si vous sélectionnez STATIQUE, entrez l'adresse IP * du réseau client*, **masque de réseau client**, **passerelle de réseau client** et **MTU du réseau client**.
- Si vous sélectionnez DHCP, l'adresse IP * du réseau client*, **masque de réseau client** et **passerelle réseau client** sont automatiquement affectées.

8. Vérifiez la configuration de l'ordinateur virtuel et apportez les modifications nécessaires.

9. Lorsque vous êtes prêt à terminer, sélectionnez **Finish** pour lancer le téléchargement de la machine virtuelle.

10. si vous avez déployé ce nœud dans le cadre d'une opération de restauration et qu'il ne s'agit pas d'une restauration de nœud complet, effectuez les opérations suivantes une fois le déploiement terminé :

- Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- Sélectionnez chaque disque dur virtuel par défaut qui a été désigné pour le stockage, puis sélectionnez **Supprimer**.

- c. En fonction de vos conditions de restauration des données, ajoutez de nouveaux disques virtuels en fonction de vos besoins de stockage, reconnectez tous les disques durs virtuels conservés sur le nœud de grille défaillant précédemment retiré, ou les deux.

Notez les consignes importantes suivantes :

- Si vous ajoutez de nouveaux disques, vous devez utiliser le même type de périphérique de stockage que celui utilisé avant la restauration du nœud.
- Le fichier .ovf de nœud de stockage définit plusieurs VMDK pour le stockage. À moins que ces VMDK ne répondent à vos besoins de stockage, vous devez les supprimer et attribuer des VMDK ou des RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus fréquemment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo).

11. si vous devez remapper les ports utilisés par ce nœud, procédez comme suit.

Il peut être nécessaire de reconfigurer un port si les politiques réseau de votre entreprise restreignent l'accès à un ou plusieurs ports utilisés par StorageGRID. Consultez "[Instructions de mise en réseau](#)" pour connaître les ports utilisés par StorageGRID.



Ne mappez pas les ports utilisés dans les terminaux d'équilibrage de charge.

- Sélectionnez la nouvelle VM.
- Dans l'onglet configurer, sélectionnez **Paramètres > Options vApp**. L'emplacement de **vApp Options** dépend de la version de vCenter.
- Dans le tableau **Propriétés**, localisez **PORT_REMAPPAGE_INBOUND** et **PORT_REMAPPAGE**.
- Pour mapper symétriquement les communications entrantes et sortantes d'un port, sélectionnez **PORT_REMAPPAGE**.



La prise en charge du remappage des ports est obsolète et sera supprimée dans une prochaine version. Pour supprimer les ports remappés, reportez-vous à "[Supprimez les mappes de ports sur les hôtes bare Metal](#)".



Si seul **PORT_REMAPPAGE** est défini, le mappage que vous spécifiez s'applique aux communications entrantes et sortantes. Si **PORT_REMAPPAGE_INBOUND** est également spécifié, **PORT_REMAPPAGE** s'applique uniquement aux communications sortantes.

- Sélectionnez **définir la valeur**.
- Saisissez le mappage de port :

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> est un grid, un admin 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_REMAPPAGE_INBOUND**.



Si vous spécifiez PORT_REMAP_INBOUND et que vous n'indiquez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées.

i. Sélectionnez **définir la valeur**.

ii. Saisissez le mappage de port :

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port  
used by grid node>
```

<network type> est un grid, un admin ou un client, et <protocol> est tcp ou udp.

Par exemple, pour remappage le trafic SSH entrant envoyé au port 3022 afin qu'il soit reçu au port 22 par le nœud de grille, entrez ce qui suit :

```
client/tcp/3022/22
```

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. Pour augmenter les valeurs par défaut du CPU ou de la mémoire du nœud :

- a. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- b. Modifiez le nombre de CPU ou la quantité de mémoire nécessaire.

Définissez la **réserve de mémoire** sur la même taille que la **mémoire** allouée à la machine virtuelle.

c. Sélectionnez **OK**.

13. Mise sous tension de la machine virtuelle

Une fois que vous avez terminé

Si vous avez déployé ce nœud dans le cadre d'une procédure d'extension ou de restauration, revenez à ces instructions pour terminer la procédure.

Exemples de fichiers de configuration pour les nœuds StorageGRID sous Linux

Vous pouvez utiliser les exemples de fichiers de configuration de nœud pour vous aider à configurer les fichiers de configuration de nœud pour votre système StorageGRID. Les exemples montrent les fichiers de configuration des nœuds pour tous les types de nœuds

grid.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

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



Dans les exemples, la cible réseau client a été configurée comme une pratique recommandée, même si le réseau client est désactivé par défaut.

Exemple pour le nœud d'administration principal

Exemple de nom de fichier : `/etc/storagegrid/nodes/dc1-adm1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Exemple de nœud de stockage

Exemple de nom de fichier : `/etc/storagegrid/nodes/dc1-sn1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour le nœud de passerelle

Exemple de nom de fichier : /etc/storagegrid/nodes/dc1-gw1.conf

Exemple de contenu de fichier:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour un nœud d'administration non primaire

Exemple de nom de fichier : /etc/storagegrid/nodes/dc1-adm2.conf

Exemple de contenu de fichier:


```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Valider la configuration StorageGRID sous Linux

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.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Pour valider le contenu des fichiers de configuration, exécutez la commande suivante sur chaque hôte :

```
sudo storagegrid node validate all
```

Si les fichiers sont corrects, le résultat indique **TRANSMIS** pour chaque fichier de configuration, comme indiqué dans l'exemple.



Lors de l'utilisation d'une seule LUN sur des nœuds de métadonnées uniquement, il se peut que vous receviez un message d'avertissement que vous pouvez ignorer.

```
Checking for misnamed node configuration files... PASSED
Checking configuration file for node dc1-adm1... PASSED
Checking configuration file for node dc1-gw1... PASSED
Checking configuration file for node dc1-sn1... PASSED
Checking configuration file for node dc1-sn2... PASSED
Checking configuration file for node dc1-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Pour une installation automatisée, vous pouvez supprimer ce résultat en utilisant les `-q` options ou de `--quiet` la `storagegrid` commande (par exemple, `storagegrid --quiet...`). Si vous supprimez la sortie, la commande aura une valeur de sortie non nulle si des avertissements ou des erreurs de configuration ont été détectés.

Si les fichiers de configuration sont incorrects, les problèmes sont affichés comme **AVERTISSEMENT** et **ERREUR**, comme indiqué dans l'exemple. Si des erreurs de configuration sont détectées, vous devez les corriger avant de poursuivre l'installation.

```
Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/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
```

Démarrez le service hôte StorageGRID sous Linux

Pour démarrer vos nœuds StorageGRID et s'assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid  
sudo systemctl start storagegrid
```

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

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

3. Si l'un des nœuds 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
```

Découvrez l'API REST d'installation de StorageGRID

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

L'API utilise la plate-forme swagger open source API pour fournir la documentation de l'API. Swagger permet aux développeurs et aux non-développeurs d'interagir avec l'API dans une interface utilisateur qui illustre la façon dont l'API répond aux paramètres et aux options. Cette documentation suppose que vous êtes familiarisé avec les technologies Web standard et le format de données JSON.



Toutes les opérations d'API que vous effectuez à l'aide de la page Web Documentation de l'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 de l'API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL requis ou facultatifs et une réponse de l'API attendue.

API d'installation de StorageGRID

L'API d'installation de StorageGRID n'est disponible que lors de la configuration initiale du système StorageGRID et si vous devez effectuer une restauration du nœud d'administration principal. L'API d'installation est accessible via HTTPS depuis le Grid Manager.

Pour accéder à la documentation de l'API, accédez à la page Web d'installation sur le nœud d'administration principal et sélectionnez **aide > documentation de l'API** dans la barre de menus.

L'API d'installation de StorageGRID comprend les sections suivantes :

- **config** : Opérations relatives à la version du produit et aux versions de l'API. Vous pouvez lister la version de la publication du produit et les versions majeures de l'API prises en charge par cette publication.
- **grid** : Opérations de configuration au niveau de la grille. Vous pouvez obtenir et mettre à jour les paramètres de la grille, notamment les détails de la grille, les sous-réseaux du réseau de la grille, les mots de passe de la grille, ainsi que les adresses IP des serveurs NTP et des serveurs DNS.
- **nœuds** : Opérations de configuration au niveau des nœuds. Vous pouvez récupérer une liste de nœuds de la grille, supprimer un nœud de la grille, configurer un nœud de la grille, afficher un nœud de la grille et réinitialiser la configuration d'un nœud de la grille.
- **provisionnement** : Opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et consulter son état.
- **Récupération** : Opérations de récupération du nœud d'administration principal. Vous pouvez réinitialiser les informations, charger le Recovery Package, démarrer la récupération et consulter l'état de l'opération de récupération.
- **recovery-package** : Opérations de téléchargement du Recovery Package.
- **Sites** : Opérations de configuration au niveau du site. Vous pouvez créer, consulter, supprimer et modifier un site.
- **mot-de-passe-temporaire** : Opérations sur le mot de passe temporaire pour sécuriser la mgmt-api pendant l'installation.

Résoudre les problèmes d'installation de StorageGRID

En cas de problème lors de l'installation de votre système StorageGRID, vous pouvez accéder aux fichiers journaux d'installation. Le support technique peut également avoir besoin d'utiliser les fichiers journaux d'installation pour résoudre les problèmes.



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Linux

Les fichiers journaux d'installation suivants sont disponibles à partir du conteneur qui exécute chaque nœud :

- `/var/local/log/install.log` (disponible sur tous les nœuds grid)
- `/var/local/log/gdu-server.log` (Disponible sur le nœud d'administration principal)

Les fichiers journaux d'installation suivants sont disponibles auprès de l'hôte :

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Pour savoir comment accéder aux fichiers journaux, reportez-vous à "[Collecte de fichiers journaux et de données système](#)" la section .

VMware

Voici les principaux fichiers journaux d'installation dont le support technique peut avoir besoin pour résoudre les problèmes.

- `/var/local/log/install.log` (disponible sur tous les nœuds grid)
- `/var/local/log/gdu-server.log` (Disponible sur le nœud d'administration principal)

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 démarrent pas.

Description de la tâche

Si vous êtes certain que l'hôte VM dispose de ressources suffisantes pour chaque nœud de la grille, ajustez manuellement les ressources allouées à chaque machine virtuelle, puis essayez de démarrer les machines virtuelles.

Étapes

1. Dans l'arborescence du client VMware vSphere Hypervisor, sélectionnez la machine virtuelle qui n'a pas démarré.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Dans la fenêtre Propriétés des machines virtuelles, sélectionnez l'onglet **Ressources**.
4. Ajustez les ressources allouées à la machine virtuelle :
 - a. Sélectionnez **CPU**, puis utilisez le curseur réservation pour régler la fréquence réservée à cette machine virtuelle.
 - b. Sélectionnez **mémoire**, puis utilisez le curseur réservation pour régler le Mo réservé pour cette machine virtuelle.
5. Sélectionnez **OK**.
6. Répétez cette procédure 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 de la machine virtuelle ou utiliser SSH avant que le nouveau nœud ne rejoigne la grille.

Si vous avez voulu 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 pour pouvoir accéder à la console ou utiliser SSH pour déboguer les problèmes d'installation.
- Utilisez vCenter pour définir le mot de passe :
 - a. Mettez la machine virtuelle hors tension.
 - b. Accédez à **VM**, sélectionnez l'onglet **configurer** et sélectionnez **vApp Options**.
 - c. Spécifiez le type de mot de passe d'installation temporaire à définir :
 - Sélectionnez **CUSTOM_TEMPORAIRES_PASSWORD** pour définir un mot de passe temporaire personnalisé.
 - Sélectionnez **TEMPORAIRES_PASSWORD_TYPE** pour utiliser le nom du nœud comme mot de passe temporaire.
 - d. Sélectionnez **définir la valeur**.
 - e. Définissez le mot de passe temporaire :
 - Remplacez **CUSTOM_TEMPORAIRES_PASSWORD** par une valeur de mot de passe personnalisée.
 - Mettez à jour **TEMPORAIRES_PASSWORD_TYPE** avec la valeur **use node name**.
 - f. Redémarrez la machine virtuelle pour appliquer le nouveau mot de passe.

Informations associées

- Pour savoir comment accéder aux fichiers journaux, reportez-vous à ["Référence des fichiers journaux"](#) la section .
- ["Dépanner un système StorageGRID"](#)
- Si vous avez besoin d'aide supplémentaire, contactez ["Support NetApp"](#).

Exemples de scripts

Exemple de consolidation de quatre interfaces physiques en une seule liaison pour StorageGRID sur RHEL

Vous pouvez utiliser ces fichiers d'exemple pour agréger quatre interfaces physiques Linux en une seule liaison LACP, puis établir trois interfaces VLAN qui fixent la liaison pour une utilisation comme interfaces réseau StorageGRID, Admin et client.

Interfaces physiques

Notez que les switches à l'autre extrémité des liaisons doivent également traiter les quatre ports comme une seule jonction ou un canal de port LACP et doivent passer au moins les trois VLAN référencés avec des balises.

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interface de liaison

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfaces VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003


```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Exemple d'agrégation d'interfaces physiques pour StorageGRID sur Ubuntu et Debian

Le `/etc/network/interfaces` fichier comprend trois sections qui définissent les interfaces physiques, l'interface de liaison et les interfaces VLAN. Vous pouvez combiner ces trois exemples de sections dans un seul fichier, qui agrège quatre interfaces physiques Linux en une seule liaison LACP, puis établir trois interfaces VLAN qui soudent le lien pour une utilisation en tant qu'interfaces réseau StorageGRID, Admin et client.

Interfaces physiques

Notez que les switches à l'autre extrémité des liaisons doivent également traiter les quatre ports comme une seule jonction ou un canal de port LACP et doivent passer au moins les trois VLAN référencés avec des balises.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interface de liaison

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfaces VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Configurer la grille et terminer l'installation

Accédez au gestionnaire de grille StorageGRID

Le gestionnaire de grille permet de définir toutes les informations nécessaires à la configuration du système StorageGRID.

Avant de commencer

Le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Étapes

1. Ouvrez votre navigateur Web et accédez à :

`https://primary_admin_node_ip`

Vous pouvez également accéder à Grid Manager sur le port 8443 :

`https://primary_admin_node_ip:8443`

Vous pouvez utiliser l'adresse IP du nœud d'administration principal sur le réseau Grid ou sur le réseau Admin, en fonction de votre configuration réseau. Vous devrez peut-être utiliser l'option Security/Advanced de votre navigateur pour accéder à un certificat non approuvé.

2. Gérer un mot de passe temporaire du programme d'installation selon les besoins :
 - Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez-le pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation
 - Pour Linux, le mot de passe a été automatiquement importé à partir du fichier de configuration du nœud à `/etc/storagegrid/nodes/<node_name>.conf`
 - Pour VMware, le mot de passe SSH/console a été automatiquement importé depuis les propriétés OVF
 - Si aucun mot de passe n'a été défini, définissez éventuellement 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 s'affiche.

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

Spécifier les informations de licence StorageGRID

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

Étapes

1. Sur la page Licence, entrez un nom significatif pour votre système StorageGRID dans le champ **Nom de la grille**.

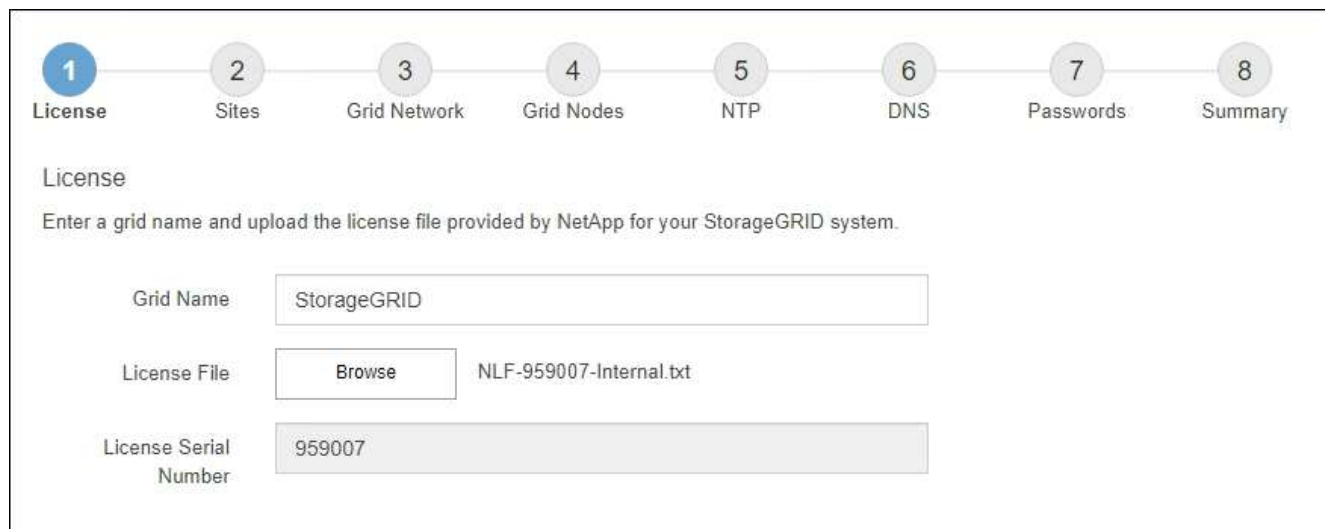
Après l'installation, le nom s'affiche en haut du menu nœuds.

2. Sélectionnez **Parcourir**, localisez le fichier de licence NetApp (*NLF-unique-id.txt*) et sélectionnez **Ouvrir**.

Le fichier de licence est validé et le numéro de série s'affiche.



L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



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**.

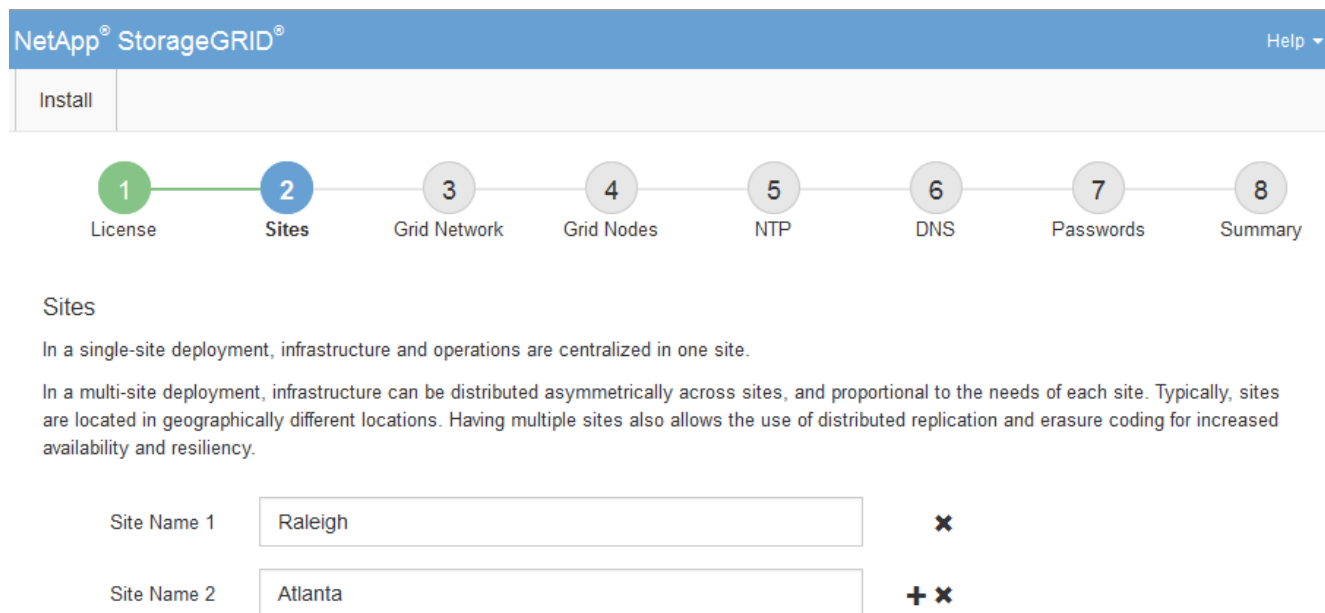
Ajouter des sites dans StorageGRID

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 **Site name**.
2. Pour ajouter d'autres sites, sélectionnez le signe plus à côté de la dernière entrée de site et saisissez le nom dans la nouvelle zone de texte **Site name**.

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. Sélectionnez **Suivant**.

Spécifiez les sous-réseaux du réseau Grid pour StorageGRID

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

Description de la tâche

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

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

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau Grid dans la zone de texte **sous-réseau 1**.
2. Sélectionnez 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, sélectionnez **Discover Grid Networks subnets** pour remplir automatiquement la liste des sous-réseaux Grid Network avec les sous-réseaux signalés par les nœuds de grille enregistrés auprès du Grid Manager.
 - Vous devez ajouter manuellement tout sous-réseau pour les serveurs NTP, DNS, LDAP ou autres serveurs externes auxquels vous accédez via la passerelle réseau Grid.

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. Sélectionnez **Suivant**.

Approuver les nœuds de grille en attente pour StorageGRID

Vous devez approuver chaque nœud de la grille pour pouvoir rejoindre le système StorageGRID.

Avant de commencer

Vous avez déployé l'ensemble des nœuds grid virtuels et d'appliance StorageGRID.



Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

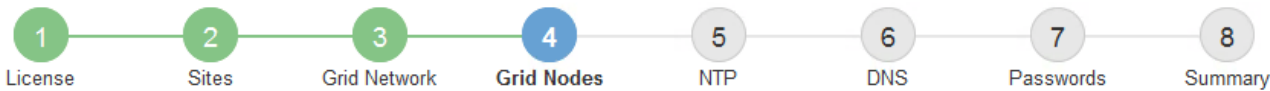
Étapes

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



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

- 2. Sélectionnez le bouton radio à côté d'un noeud 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. Sélectionnez **approuver**.
- 4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :
 - **Site** : le nom système du site pour ce noeud de grille.
 - **Nom** : le nom du système pour le noeud. Le nom par défaut est le nom que vous avez spécifié lors de la configuration du nœud.

Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés une fois l'installation terminée. Cependant, au cours de cette étape du processus

d'installation, vous pouvez modifier les noms de système selon vos besoins.



Pour un noeud VMware, vous pouvez changer le nom ici, mais cette action ne changera pas le nom de la machine virtuelle dans vSphere.

- **NTP role** : rôle NTP (Network Time Protocol) du noeud de la grille. Les options sont **automatique**, **primaire** et **client**. Si vous sélectionnez **automatique**, le rôle principal est attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille ayant des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.



Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

- **Type de stockage** (noeuds de stockage uniquement) : spécifiez qu'un nouveau noeud de stockage doit être utilisé exclusivement pour les données uniquement, les métadonnées uniquement ou les deux. Les options sont **données et métadonnées** ("combinées"), **données seulement** et **métadonnées seulement**.



Pour plus d'informations sur les exigences relatives à ces types de nœuds, reportez-vous à la section "[Types de nœuds de stockage](#)".

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

5. Dans le réseau de grille, modifiez les paramètres des propriétés suivantes si nécessaire :

- **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface Grid Network (eth0 dans le conteneur). Par exemple : 192.168.1.234/21
- **Gateway** : la passerelle réseau Grid. Par exemple : 192.168.0.1

La passerelle est requise en cas de sous-réseaux de grille multiples.



Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne fait pas partie d'un pool d'adresses DHCP.

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

Entrez les sous-réseaux de destination des routes en dehors de cette interface dans la zone de texte **sous-réseaux (CIDR)**. En cas de sous-réseaux d'administration multiples, la passerelle d'administration est requise.



Si vous avez sélectionné DHCP pour la configuration du réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne fait pas partie d'un pool d'adresses DHCP.

Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

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

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **configurer réseau > Configuration lien** et activez les réseaux appropriés.
- c. Sélectionnez **configurer réseau > Configuration IP** et configurez les réseaux activés.
- d. Retournez à la page d'accueil et sélectionnez **Démarrer l'installation**.
- e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.
- f. Supprimez le nœud du tableau nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, reportez-vous au ["Démarrage rapide pour l'installation du matériel"](#) pour 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 en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne fait pas partie d'un pool d'adresses DHCP.

Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

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

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **configurer réseau > Configuration lien** et activez les réseaux appropriés.
- c. Sélectionnez **configurer réseau > Configuration IP** et configurez les réseaux activés.
- d. Retournez à la page d'accueil et sélectionnez **Démarrer l'installation**.

- e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.
- f. Supprimez le nœud du tableau nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, reportez-vous au ["Démarrage rapide pour l'installation du matériel"](#) pour localiser les instructions relatives à votre appareil.

8. Sélectionnez **Enregistrer**.

L'entrée de nœud de la grille passe à la liste 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.

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 à approuver.

Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de sélectionner **Installer** sur la page Résumé. Vous pouvez modifier les propriétés d'un nœud de grille approuvé en sélectionnant son bouton radio et en sélectionnant **Modifier**.

10. Une fois que vous avez terminé d'approuver les nœuds de la grille, sélectionnez **Suivant**.

Spécifiez les informations du serveur Network Time Protocol pour StorageGRID

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

Description de la tâche

Vous devez indiquer des adresses IPv4 pour les serveurs NTP.

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

Vous devez spécifier quatre références de serveur NTP de Stratum 3 ou supérieur pour éviter les problèmes de dérive du temps.



Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service heure Windows (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

["Limite de support pour une heure de haute précision"](#)

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



Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

(VMware uniquement) Effectuez des vérifications supplémentaires pour VMware, par exemple en vous assurant que l'hyperviseur utilise la même source NTP que la machine virtuelle et en utilisant VMTools pour désactiver la synchronisation horaire entre l'hyperviseur et les machines virtuelles StorageGRID .

Étapes

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

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 associées

["Instructions de mise en réseau"](#)

Spécifiez les informations du serveur DNS pour StorageGRID

Vous devez spécifier des informations DNS pour votre système StorageGRID afin de pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

Description de la tâche

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

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

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Étapes

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

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 indiquer jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe système StorageGRID

Dans le cadre de l'installation de votre système StorageGRID, vous devez saisir les mots de passe à utiliser pour sécuriser votre système et effectuer des tâches de maintenance.

Description de la tâche

Utilisez la page installer des mots de passe pour spécifier le mot de passe de provisionnement et le mot de passe utilisateur root de la gestion de grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID.
- Vous devez disposer du mot de passe de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du progiciel de restauration. Il est donc important de stocker la phrase secrète de provisionnement dans un emplacement sécurisé.
- Vous pouvez modifier la phrase de passe de provisionnement à partir de Grid Manager si vous en avez la version actuelle.
- Le mot de passe de l'utilisateur root de la gestion de grille peut être modifié à l'aide de Grid Manager.
- Les mots de passe SSH et la console de ligne de commande générés de manière aléatoire sont stockés dans `Passwords.txt` le fichier du progiciel de récupération.

Étapes

1. Dans **Phrase secrète de provisionnement**, saisissez la phrase secrète de provisionnement qui sera nécessaire pour apporter des modifications à la topologie de la grille de votre système StorageGRID.

Stockez la phrase secrète de provisionnement dans un endroit sécurisé.



Si, une fois l'installation terminée, 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 grille**.

2. Dans **Confirmer la phrase secrète de provisionnement**, saisissez à nouveau la phrase secrète de provisionnement pour la confirmer.
3. Dans **Grid Management Root User Password**, entrez le mot de passe à utiliser pour accéder au Grid Manager en tant qu'utilisateur « root ».



Stockez la phrase secrète de provisionnement dans un endroit sûr. Il est nécessaire pour les procédures d'installation, d'extension et de maintenance.

4. Dans **confirmer le mot de passe de l'utilisateur racine**, entrez à nouveau le mot de passe de Grid Manager 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.

5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désactivez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

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



Vous êtes invité à télécharger le fichier Recovery Package (sgws-recovery-package-id-revision.zip) après avoir sélectionné **Installer** sur la page Résumé. Vous devez ["téléchargez ce fichier"](#) pour terminer l'installation. Les mots de passe nécessaires pour accéder au système sont stockés dans le fichier Passwords.txt, contenu dans le fichier Recovery Package.

6. Sélectionnez **Suivant**.

Vérifiez la configuration de votre StorageGRID

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

Étapes

1. Afficher la page **Résumé**.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

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

Modify Grid Nodes

Raleigh

dc1-adm1

dc1-g1

dc1-s1

dc1-s2

dc1-s3

NetApp-SGA

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

3. Sélectionnez **Installer**.



Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud bascule du réseau Grid vers le réseau client lorsque vous sélectionnez **Installer**. Si vous perdez la connectivité, vous devez vous assurer que vous accédez au nœud d'administration principal via un sous-réseau accessible. Voir "[Instructions de mise en réseau](#)" pour plus de détails.

4. Sélectionnez **Télécharger le paquet de récupération**.

Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (.zip) et à confirmer que vous pouvez accéder au contenu de ce fichier. Vous devez télécharger le fichier Recovery Package afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou de plusieurs nœuds de la grille. L'installation se poursuit en arrière-plan, mais vous ne pouvez pas terminer l'installation et accéder au système

StorageGRID tant que vous n'avez pas téléchargé et vérifié ce fichier.

5. Vérifiez que vous pouvez extraire le contenu du .zip fichier, puis l'enregistrer dans deux emplacements sûrs, sécurisés et séparés.



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

6. Cochez la case **J'ai téléchargé et vérifié avec succès le fichier du Recovery Package**, puis sélectionnez **Suivant**.

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

Installation Status

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

Search					
Name	Site	Grid Network IPv4 Address	Progress	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 complète est atteinte pour tous les nœuds de la grille, la page de connexion de Grid Manager s'affiche.

7. Connectez-vous au gestionnaire de grille à l'aide de l'utilisateur « root » et du mot de passe que vous avez spécifié lors de l'installation.

Exigences réseau et DHCP après l'installation de StorageGRID

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

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

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



Les nœuds redémarrent lorsque la configuration Grid Network 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 Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un nœud de grille. Voir "[Configurez les adresses IP](#)".
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Découvrez les étapes obligatoires et facultatives après l'installation de StorageGRID

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

Tâches requises

- (VMware uniquement) Configurez VMware vSphere Hypervisor pour le redémarrage automatique.

Vous devez configurer l'hyperviseur pour redémarrer les machines virtuelles lorsque le serveur redémarre. Sans redémarrage automatique, les machines virtuelles et les nœuds de la grille restent arrêtés après le redémarrage du serveur. Pour en savoir plus, consultez la documentation relative à l'hyperviseur VMware vSphere.

- ["Créez un compte de locataire"](#) Il s'agit du protocole client S3 qui sera utilisé pour stocker des objets sur votre système StorageGRID.
- ["Contrôler l'accès au système"](#) en configurant des groupes et des comptes utilisateur. Vous pouvez également ["configurer un référentiel d'identité fédéré"](#) (par exemple, Active Directory ou OpenLDAP), afin de pouvoir importer des groupes et des utilisateurs d'administration. Ou, vous pouvez ["créer des groupes et des utilisateurs locaux"](#).
- Intégrez et testez les ["API S3"](#) applications client que vous utiliserez pour télécharger des objets sur votre système StorageGRID.
- ["Configuration des règles de gestion du cycle de vie des informations \(ILM\) et de la règle ILM"](#) utilisez pour protéger les données d'objet.
- Si votre installation inclut des nœuds de stockage de l'appliance, effectuez les tâches suivantes avec SANtricity OS :
 - Connectez-vous à chaque appliance StorageGRID.
 - Vérifiez la réception des données AutoSupport.

Voir ["Configurer le matériel"](#).

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

Tâches facultatives

- ["Mettre à jour les adresses IP des nœuds de la grille"](#) s'ils ont changé depuis que vous avez planifié votre déploiement et généré le package de récupération.
- ["Configurer le chiffrement du stockage"](#), si nécessaire.
- ["Configurer la compression du stockage"](#) pour réduire la taille des objets stockés, si nécessaire.
- ["Configurez les interfaces VLAN"](#) pour isoler et partitionner le trafic réseau, le cas échéant.
- ["Configurez les groupes haute disponibilité"](#) Pour améliorer la disponibilité de la connexion des clients Grid Manager, tenant Manager et S3, si nécessaire.
- ["Configurer les terminaux de l'équilibreur de charge"](#) Pour la connectivité client S3, si nécessaire.

Mettez à niveau le logiciel StorageGRID

Mettez à niveau le logiciel StorageGRID

Suivez 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.



Ne démarrez pas la mise à niveau si vous avez un besoin urgent d'étendre votre stockage pour augmenter la capacité (si votre stockage est presque plein). Terminez la procédure de mise à niveau en temps opportun. Si une récupération est nécessaire, contactez le support technique.

Avant de procéder à la mise à niveau

Consultez ces rubriques pour découvrir les nouvelles fonctionnalités et améliorations de StorageGRID 12.1, déterminer si certaines fonctionnalités ont été dépréciées ou supprimées et vous renseigner sur les modifications apportées aux API StorageGRID.

- ["Quel est l'impact de votre système pendant la mise à niveau"](#)
- ["Nouveautés de StorageGRID 12.1"](#)
- ["Fonctions supprimées ou obsolètes"](#)
- ["Modifications apportées à l'API de gestion du grid"](#)
- ["Modifications apportées à l'API de gestion des locataires"](#)

Planifiez et préparez la mise à niveau

Estimez le temps nécessaire pour effectuer une mise à niveau de StorageGRID

Réfléchissez au moment opportun pour effectuer une mise à niveau, en fonction du temps nécessaire. Soyez conscient des opérations que vous pouvez et ne pouvez pas effectuer à chaque étape de la mise à niveau.

Description de la tâche

Le temps nécessaire à une mise à niveau d'StorageGRID dépend de divers facteurs, tels que la charge client et les performances matérielles.

Le tableau résume les principales tâches de mise à niveau et indique le temps approximatif requis pour chaque tâche. Les étapes qui suivent le tableau fournissent des instructions que vous pouvez utiliser pour estimer le temps de mise à niveau de votre système.

Tâche de mise à niveau	Description	Temps approximatif requis	Au cours de cette tâche
Exécutez des contrôles préalables et mettez à niveau le nœud d'administration principal	Les précontrôles de mise à niveau sont exécutés et le nœud d'administration principal est arrêté, mis à niveau et redémarré.	de 30 minutes à 1 heure, avec les nœuds d'appliance de services qui demandent le plus de temps. Les erreurs de vérification préalable non résolues augmentent ce temps.	Vous ne pouvez pas accéder au nœud d'administration principal. Des erreurs de connexion peuvent être signalées, que vous pouvez ignorer. L'exécution des contrôles préalables à la mise à niveau avant le démarrage de la mise à niveau vous permet de résoudre les erreurs avant la fenêtre de maintenance de mise à niveau planifiée.
Démarrez le service de mise à niveau	Le fichier logiciel est distribué et le service de mise à niveau démarre.	3 minutes par nœud de grid	
Mettez à niveau les autres nœuds grid	Le logiciel sur tous les autres nœuds de grille est mis à niveau dans l'ordre dans lequel vous approuvez les nœuds. Un nœud d'administration ou de passerelle est mis à niveau en même temps qu'un nœud de stockage.	de 15 minutes à 1 heure par nœud, avec des nœuds d'appliance exigeant le plus de temps Remarque : pour les nœuds d'appliance, le programme d'installation de l'appliance StorageGRID est automatiquement mis à jour vers la dernière version.	• Ne modifiez pas la configuration de la grille. • Ne modifiez pas la configuration du niveau d'audit. • Ne mettez pas à jour la configuration ILM. • Vous n'êtes pas en mesure d'effectuer d'autres procédures de maintenance, comme le correctif, la mise hors service ou l'extension. Remarque : si vous devez effectuer une récupération, contactez le support technique.
Activer les fonctions	Les nouvelles fonctionnalités de la nouvelle version sont activées.	Jusqu'à 1 heure	• 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.
Dernières étapes de mise à niveau	Les fichiers temporaires sont supprimés et la mise à niveau vers la nouvelle version se termine.	5 minutes	Lorsque la tâche étapes finales de mise à niveau est terminée, vous pouvez effectuer toutes les procédures de maintenance.

Estimer le temps de mise à niveau

Étapes

1. Estimez le temps nécessaire à la mise à niveau de tous les nœuds du grid.
 - a. Multipliez par 1 heure/nœud le nombre de nœuds de votre système StorageGRID.

En règle générale, les nœuds d'appliance sont plus longs à mettre à niveau que les nœuds basés sur logiciel.

 - b. Ajoutez 1 heure à cette heure pour tenir compte du temps nécessaire au téléchargement du `.upgrade` fichier, exécuter des validations de précontrôle et terminer les étapes finales de mise à niveau.
2. Si vous avez des nœuds Linux, ajoutez 15 minutes pour chaque nœud afin de tenir compte du temps nécessaire au téléchargement et à l'installation du package RPM ou DEB.
3. Calculer le temps total estimé pour la mise à niveau en ajoutant les résultats des étapes 1 et 2.

Exemple : Temps estimé pour la mise à niveau vers StorageGRID 12.1

Supposons que votre système dispose de 14 nœuds de grille, dont 8 sont des nœuds Linux.

1. Multipliez 14 par 1 heure/nœud.
2. Ajoutez 1 heure pour prendre en compte les étapes de téléchargement, de vérification préalable et finales.

La durée estimée de mise à niveau de tous les nœuds est de 15 heures.

3. Multipliez 8 par 15 minutes/nœud pour tenir compte du temps nécessaire à l'installation du package RPM ou DEB sur les nœuds Linux.

La durée estimée de cette étape est de 2 heures.

4. Ajoutez les valeurs ensemble.

Vous devriez prévoir jusqu'à 18 heures pour terminer la mise à niveau de votre système vers StorageGRID 12.1.0.



Si nécessaire, vous pouvez diviser la fenêtre de maintenance en fenêtres plus petites en approuvant des sous-ensembles de nœuds de grille pour la mise à niveau dans plusieurs sessions. Par exemple, vous pouvez préférer mettre à niveau les nœuds sur le site A en une session, puis mettre à niveau les nœuds sur le site B dans une session ultérieure. Si vous choisissez d'effectuer la mise à niveau dans plusieurs sessions, sachez que vous ne pouvez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'ont pas été mis à niveau.

Comment les mises à niveau de StorageGRID affectent votre système

Découvrez les conséquences sur votre système StorageGRID lors de la mise à niveau.

L'accès SSH externe est autorisé jusqu'à la fin de la mise à niveau

L'accès SSH externe est autorisé pendant la mise à niveau. Une fois la mise à niveau terminée, l'accès SSH externe est bloqué par défaut. Après la mise à niveau, vous pouvez utiliser l'onglet **Bloquer SSH** disponible sur la page **Gestionnaire de grille > Paramètres de sécurité** pour "[gérer l'accès SSH externe](#)". L'accès SSH

entre les nœuds de la grille n'est pas affecté.

Les mises à niveau de StorageGRID ne générant pas de perturbation

Le système StorageGRID peut ingérer et récupérer les données depuis les applications client tout au long du processus de mise à niveau. Si vous approuvez la mise à niveau de tous les nœuds du même type (par exemple, nœuds de stockage), les nœuds sont arrêtés un par un. Ainsi, il n'y a pas de temps lorsque tous les nœuds de grid ou tous les nœuds de grid d'un certain type sont indisponibles.

Pour assurer une disponibilité continue, vérifiez que votre règle ILM contient des règles qui spécifient le stockage de plusieurs copies de chaque objet. Vous devez également vous assurer que tous les clients S3 externes sont configurés pour envoyer des demandes à l'un des éléments suivants :

- Adresse IP virtuelle d'un groupe haute disponibilité (HA)
- Équilibreur de charge tiers haute disponibilité
- Plusieurs nœuds de passerelle pour chaque client
- Plusieurs nœuds de stockage pour chaque client

Les applications client peuvent subir des interruptions à court terme

Le système StorageGRID peut ingérer et récupérer des données provenant des applications client tout au long du processus de mise à niveau. Toutefois, les connexions client vers des nœuds de passerelle ou de stockage individuels peuvent être interrompues temporairement si la mise à niveau doit redémarrer des 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'indisponibilité pour effectuer une mise à niveau si une perte de connectivité pendant une courte période n'est pas acceptable. Vous pouvez utiliser l'approbation sélective pour planifier la mise à jour de certains nœuds.



Vous pouvez utiliser plusieurs passerelles et groupes haute disponibilité pour assurer le basculement automatique lors du processus de mise à niveau. Voir les instructions pour ["configuration des groupes haute disponibilité"](#).

Les réparations en arrière-plan ne s'exécuteront pas sur les grilles avec des nœuds de versions mixtes

Les réparations en arrière-plan ne s'exécutent pas pendant la mise à niveau lorsque la grille contient des nœuds de versions mixtes. Les incohérences qui surviennent lors d'une panne de site ne seront pas réparées tant que la mise à niveau n'est pas terminée.

Le micrologiciel de l'appliance est mis à niveau

Lors de la mise à niveau de StorageGRID 12.1 :

- Tous les nœuds d'appliance StorageGRID sont automatiquement mis à niveau vers la version 12.1 du firmware StorageGRID Appliance Installer.
- Les appareils SG6060 et SGF6024 sont automatiquement mis à niveau vers la version 3B08.EX du micrologiciel du BIOS et la version 4.01.07 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 4.75.07 du micrologiciel BMC .
- Les appliances SGF6112, SG6160, SG110 et SG1100 sont automatiquement mises à niveau vers la version 3A14.QD du firmware BIOS et la version 3.21.07 du firmware BMC.

Les règles ILM sont gérées différemment en fonction de leur état

- La stratégie active reste la même après la mise à niveau.
- Seules les 10 dernières règles historiques sont conservées lors de la mise à niveau.
- Si une stratégie est proposée, elle sera supprimée lors de la mise à niveau.

Il est possible que des alertes soient déclenchées

Des alertes peuvent être déclenchées lorsque les services démarrent et s'arrêtent, et lorsque le système StorageGRID fonctionne comme un environnement de version mixte (certains nœuds de grid exécutant une version antérieure, alors que d'autres ont été mis à niveau vers une version plus récente). D'autres alertes peuvent être déclenchées une fois la mise à niveau terminée.

Par exemple, l'alerte « Impossible de communiquer avec le nœud » peut s'afficher lorsque les services sont arrêtés, ou l'alerte « Erreur de communication Cassandra » peut apparaître lorsque certains nœuds ont été mis à niveau vers StorageGRID 12.0 ou une version ultérieure, tandis que d'autres exécutent encore une version antérieure de StorageGRID. En général, ces alertes disparaissent une fois la mise à niveau terminée.

L'alerte « Placement ILM impossible » peut être déclenchée lorsque des nœuds de stockage sont arrêtés pendant la mise à niveau vers StorageGRID 12.0 ou une version ultérieure. 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 de Grid Manager.

Les modifications de configuration sont restreintes



Les restrictions relatives aux modifications de configuration sont spécifiques à chaque version. Si vous effectuez une mise à niveau vers une autre version de StorageGRID, veuillez consulter la liste des modifications interdites dans les instructions de mise à niveau de cette version.

Jusqu'à la fin de la tâche **Activer la nouvelle fonction** :

- N'apportez aucune modification à la configuration de la grille.
- N'activez ou ne désactivez aucune nouvelle fonctionnalité.
- Ne mettez pas à jour la configuration ILM. Sinon, vous risquez d'avoir un comportement ILM incohérent et inattendu.
- N'appliquez pas de correctif ou ne restaurez pas de nœud de grille.



Contactez le support technique si vous avez besoin de restaurer un nœud pendant la mise à niveau.

- 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.
- Ne supprimez aucun groupe HA tant que la mise à niveau n'est pas terminée. Les adresses IP virtuelles des autres groupes HA pourraient devenir inaccessibles.

Jusqu'à la fin de la tâche **étapes de mise à niveau finale** :

- N'effectuez pas de procédure d'extension.
- N'effectuez pas de procédure de mise hors service.

Vérifiez la version installée de StorageGRID avant la mise à niveau

Avant de démarrer la mise à niveau, vérifiez que la version précédente de StorageGRID est actuellement installée avec le dernier correctif disponible appliqué.

Description de la tâche

Avant de passer à StorageGRID 12.1, votre grid doit avoir StorageGRID 12.0 ou une version ultérieure installée. 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 grid soit au moins StorageGRID 12.0.0.

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. Se référer à "[Téléchargement NetApp : StorageGRID](#)" et les notes de publication de chaque correctif pour en savoir plus.

Vérifier la version installée

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
2. Dans le haut du Gestionnaire de grille, sélectionnez **aide** > **About**.
3. Vérifiez que la **Vers**ion est 11.9.0.8 ou une version ultérieure.
4. Si la **Vers**ion n'est pas 11.9.0.8 ou une version ultérieure, accédez à "[Téléchargement NetApp : StorageGRID](#)" pour télécharger les fichiers de mise à niveau et de correctifs dont vous avez besoin.
5. "[Suivez les instructions de mise à niveau](#)" pour chaque version que vous avez téléchargée. "[Appliquez le dernier correctif](#)" pour chaque version (fortement recommandé).

Reportez-vous à l'exemple de mise à niveau suivant.

Exemple : Mise à niveau vers StorageGRID 12.0 à partir de la version 11.8

L'exemple suivant illustre les étapes de mise à niveau de StorageGRID de la version 11.9 à la version 12.0 en préparation d'une mise à niveau vers StorageGRID 12.1.

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 11.8.0.
2. Appliquez le dernier correctif StorageGRID 11.8.0.y.
3. Mise à niveau vers la version majeure de StorageGRID 11.9.0.
4. Appliquez le correctif StorageGRID 11.9.0.8 ou version ultérieure.

Obtenez les éléments nécessaires pour une mise à niveau du logiciel StorageGRID

Avant de commencer la mise à niveau du logiciel, procurez-vous tous les documents nécessaires.

Élément	Remarques
L'ordinateur portable de service	L'ordinateur portable de service doit posséder : • Port réseau • Client SSH (par exemple, PuTTY)
"Navigateur Web pris en charge"	La prise en charge des navigateurs a généralement été modifiée pour chaque version de StorageGRID. Assurez-vous que votre navigateur est compatible avec la nouvelle version de StorageGRID.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas répertoriée dans le <code>Passwords.txt</code> fichier.
Archive RPM ou DEB Linux	Si des nœuds sont déployés sur des hôtes Linux, vous devez d' "Téléchargez et installez le progiciel RPM ou DEB sur tous les hôtes" abord démarrer la mise à niveau. Assurez-vous que votre système d'exploitation Linux répond aux exigences minimales de version du noyau de StorageGRID. Voir "Installer StorageGRID sur les hôtes Linux" .
Documentation StorageGRID	• "Notes de mise à jour". Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version. Veuillez les lire attentivement avant de procéder à la mise à niveau. • "Guide de résolution des mises à niveau logicielles StorageGRID" pour la version majeure vers laquelle vous effectuez la mise à niveau (connexion requise) • Autre "Documentation StorageGRID", selon les besoins.

Vérifiez l'état de votre système StorageGRID avant la mise à niveau

Avant de mettre à niveau un système StorageGRID, vérifiez que le système est prêt pour la mise à niveau. Vérifiez que le système fonctionne normalement et que tous les nœuds de grid sont opérationnels.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Recherchez et résolvez les alertes actives.
3. Reportez-vous à ["Communications internes sur les nœuds de la grille"](#) et ["Communications externes"](#) pour vous assurer que tous les ports requis pour StorageGRID 12.1 sont ouverts avant la mise à niveau.



Aucun port supplémentaire n'est requis lors de la mise à niveau vers StorageGRID 12.1.

Mise à niveau du logiciel

Démarrage rapide pour les mises à niveau de StorageGRID

Avant de commencer la mise à niveau, passez en revue le workflow général. La page mise à niveau de StorageGRID vous guide à chaque étape de la mise à niveau.

1

Préparez les hôtes Linux

Si des nœuds StorageGRID sont déployés sur des hôtes Linux, "[Installez le package RPM ou DEB sur chaque hôte](#)" avant de démarrer la mise à niveau.

2

Téléchargez les fichiers de mise à niveau et de correctif

Depuis le nœud d'administration principal, accédez à la page mise à niveau StorageGRID et téléchargez le fichier de mise à niveau et le fichier correctif, si nécessaire.

3

Télécharger le package de récupération

Téléchargez le package de récupération actuel avant de commencer la mise à niveau.

4

Exécuter des précontrôles de mise à niveau

Les précontrôles de mise à niveau vous aident à détecter les problèmes, de sorte que vous pouvez les résoudre avant de commencer la mise à niveau réelle.

5

Démarrer la mise à niveau

Lorsque vous démarrez la mise à niveau, les précontrôles sont à nouveau exécutés et le nœud d'administration principal est mis à niveau automatiquement. Vous ne pouvez pas accéder au gestionnaire de grille pendant la mise à niveau du nœud d'administration principal. Les journaux d'audit seront également indisponibles. Cette mise à niveau peut prendre jusqu'à 30 minutes.

6

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 grid individuels, des groupes de nœuds grid ou tous les nœuds.



N'approuvez pas la mise à niveau d'un nœud grid sauf si vous êtes sûr que ce nœud est prêt à être arrêté et redémarré.

8

Reprendre les opérations

Une fois tous les nœuds de la grille mis à niveau, de nouvelles fonctionnalités sont activées et vous pouvez reprendre les opérations. Vous devez attendre d'effectuer une procédure de mise hors service ou d'extension jusqu'à ce que la tâche d'arrière-plan **mettre à niveau la base de données** et la tâche **étapes finales de mise à niveau** soient terminées.

Informations associées

["Estimer le temps nécessaire pour effectuer une mise à niveau"](#)

Téléchargez et installez les paquets RPM ou DEB sur tous les hôtes Linux pour StorageGRID

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.

Téléchargez les fichiers de mise à niveau, Linux et de correctif

Lorsque vous effectuez une mise à niveau StorageGRID à partir du Gestionnaire de grille, vous êtes invité à télécharger l'archive de mise à niveau et tout correctif requis dans la première étape. Cependant, si vous devez télécharger des fichiers pour mettre à niveau les hôtes Linux, vous pouvez gagner du temps en téléchargeant à l'avance tous les fichiers requis.

Étapes

1. Allez à ["Téléchargement NetApp : StorageGRID"](#).
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.

Les versions du logiciel StorageGRID ont le format suivant : 11.x.y. Les correctifs StorageGRID ont le format suivant : 11.x.y.z.

3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Si un avertissement attention/MustRead apparaît, notez le numéro du correctif et cochez la case.
5. Lisez le contrat de licence de l'utilisateur final (CLUF), cochez la case, puis sélectionnez **accepter et continuer**.

La page des téléchargements de la version sélectionnée s'affiche. La page contient trois colonnes.

6. A partir de la deuxième colonne (**Upgrade StorageGRID**), téléchargez deux fichiers :
 - L'archive de mise à niveau pour la dernière version (il s'agit du fichier dans la section intitulée **VMware, SG1000 ou SG100 Primary Admin Node**). Ce fichier n'est pas nécessaire tant que vous n'avez pas effectué la mise à niveau, mais le téléchargement de ce fichier permet de gagner du temps.
 - Une archive RPM ou DEB .tgz au format ou .zip. Sélectionnez le .zip fichier si vous exécutez Windows sur l'ordinateur portable de service.

- **RHEL**

- StorageGRID-Webscale-version-RPM-uniqueID.zip
 - StorageGRID-Webscale-version-RPM-uniqueID.tgz

- **Ubuntu ou Debian +**

- StorageGRID-Webscale-version-DEB-uniqueID.zip
 - StorageGRID-Webscale-version-DEB-uniqueID.tgz

7. Si vous devez accepter un avis attention/MustRead en raison d'un correctif requis, téléchargez le correctif :

- a. Revenir à ["Téléchargement NetApp : StorageGRID"](#).
- b. Sélectionnez le numéro de correctif dans la liste déroulante.
- c. Acceptez à nouveau la mise en garde et le CLUF.
- d. Téléchargez et enregistrez le correctif et son fichier README.

Vous serez invité à télécharger le fichier de correctif sur la page mise à niveau StorageGRID lorsque vous démarrez la mise à niveau.

8. La vérification de la signature du code est manuelle sur un nœud Linux. En option, vérifiez l'archive d'installation :
 - a. Téléchargez le package de vérification de signature de code StorageGRID. Le nom de fichier de ce module 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 ["vérifiez manuellement les fichiers d'installation"](#).

Installez l'archive sur tous les hôtes Linux

Procédez comme suit avant de mettre à niveau le logiciel StorageGRID.

Étapes

1. Extrayez les packages RPM ou DEB du fichier d'installation.
2. Installez les packages RPM ou DEB sur tous les hôtes Linux.

Consultez les étapes d'installation des services hôtes StorageGRID pour Linux dans ["Installez les services d'hôte StorageGRID"](#).

Les nouveaux packages sont installés en tant que modules 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 StorageGRID.

RHEL

1. Capturer 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 que 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. Capturer 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 que 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. Supprimer les images du conteneur StorageGRID.

Docker

1. Capturer la liste des images de conteneur installées : `docker images`

Exemple :

```
[root@docker-example ~]# docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED
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 des 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 que 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. Capturer la liste des images de conteneur installées : `podman images`

Exemple :

```
[root@podman-example ~]# podman images
REPOSITORY                                TAG          IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0             Storage_Node  7125480de71b  7 months
ago    2.57 GB
localhost/storagegrid-11.8.0             Admin_Node   404e9f1bd173  7 months
ago    2.67 GB
localhost/storagegrid-11.8.0             Archive_Node c3294a29697c  7 months
ago    2.42 GB
localhost/storagegrid-11.8.0             API_Gateway  1f88f24b9098  7 months
ago    1.77 GB
localhost/storagegrid-11.7.0             Storage_Node 1655350eff6f  16 months
ago    2.54 GB
localhost/storagegrid-11.7.0             Admin_Node   872258dd0dc8  16 months
ago    2.51 GB
localhost/storagegrid-11.7.0             Archive_Node 121e7c8b6d3b  16 months
ago    2.44 GB
localhost/storagegrid-11.7.0             API_Gateway  5b7a26e382de  16 months
ago    1.8 GB
localhost/storagegrid-11.6.0             Admin_Node   ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0             Storage_Node f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0             Archive_Node 5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0             API_Gateway  cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. Supprimez les images de conteneur des 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 que 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 ~]#
```

Effectuez une mise à niveau de StorageGRID

Vous pouvez mettre à niveau vers StorageGRID 12.1 et appliquer le correctif le plus récent 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 passé en revue toutes les considérations et terminé toutes les étapes de planification et de préparation.



Ne démarrez pas la mise à niveau si vous avez un besoin urgent d'étendre votre stockage pour augmenter la capacité (si votre stockage est presque plein). Terminez la procédure de mise à niveau en temps opportun. Si une récupération est nécessaire, contactez le support technique.

Accédez à la page mise à niveau StorageGRID

Dans un premier temps, accédez à la page mise à niveau StorageGRID dans le Gestionnaire de grille.

Étapes

1. Connectez-vous au Gestionnaire de grille 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 StorageGRID, sélectionnez **mettre à niveau**.

Sélectionnez fichiers

Le chemin de mise à jour sur la page de mise à niveau StorageGRID indique quelles versions majeures (par exemple, 12.1.0) et quels correctifs (par exemple, 12.1.0.1) 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 des fichiers**, vérifiez le chemin de mise à jour.
2. Dans la section Télécharger les fichiers, sélectionnez chaque lien **Télécharger** pour télécharger les fichiers requis depuis le site de support NetApp.

Si aucun chemin de mise à jour n'est affiché, rendez-vous sur le ["Téléchargement NetApp : StorageGRID"](#) pour déterminer si une nouvelle version ou un correctif est disponible et pour télécharger les fichiers dont vous avez besoin.



Si vous avez besoin de télécharger et d'installer un package RPM ou DEB sur tous les hôtes Linux, il se peut que vous ayez déjà répertorié les fichiers de mise à niveau et de correctif StorageGRID dans le chemin de mise à jour.

3. Sélectionnez **Parcourir** pour télécharger le fichier de mise à niveau de version sur StorageGRID :
`NetApp_StorageGRID_12.1.0_Software_uniqueID.upgrade`

Une fois le téléchargement et la vérification de la signature du code terminés, une coche verte apparaît à côté du nom du fichier.

4. Si vous avez téléchargé un fichier correctif, sélectionnez **Parcourir** pour télécharger ce fichier. Le correctif sera automatiquement appliqué dans le cadre de la mise à niveau de la version.
5. Sélectionnez **Continuer**.

Exécutez des contrôles préalables

L'exécution de contrôles préalables vous permet de détecter et de résoudre les problèmes de mise à niveau avant de commencer à mettre à niveau votre grille.

Étapes

1. Pour l'étape **Exécuter les précontrôles**, commencez par saisir la phrase de passe de provisionnement pour votre grille.
2. Sélectionnez **Télécharger le paquet de récupération**.

Vous devez télécharger la copie actuelle du fichier du package de récupération avant de mettre à niveau le nœud d'administration principal. Le fichier de package de récupération vous permet de restaurer le système en cas de panne.

3. Une fois le fichier téléchargé, vérifiez que vous pouvez y accéder, y compris le `Passwords.txt` fichier.
4. Copiez le fichier téléchargé (.zip) dans deux emplacements 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 du système StorageGRID .

5. Sélectionnez **Exécuter les précontrôles** et attendez que les précontrôles soient terminés.
6. Examinez les détails de chaque vérification préalable signalée et corrigez toute erreur signalée. Consultez la "[Guide de résolution des mises à niveau logicielles StorageGRID](#)" pour la version StorageGRID 12.1.

Vous devez résoudre tous les problèmes de vérification préalable *erreurs* avant de pouvoir mettre à niveau votre système. Cependant, vous n'avez pas besoin de corriger les *avertissements* de prévérification avant de procéder à la mise à niveau.



Si vous avez ouvert des ports de pare-feu personnalisés, vous êtes averti lors de la validation de contrôle préalable. Vous devez contacter le support technique avant de procéder à la mise à niveau.

7. Si vous avez apporté des modifications à la configuration pour résoudre les problèmes signalés, sélectionnez **Exécuter les contrôles préalables** à nouveau pour obtenir des résultats mis à jour.

Si toutes les erreurs ont été résolues, vous êtes invité à démarrer la mise à niveau.

Démarrez la mise à niveau et mettez à niveau le nœud d'administration principal

Lorsque vous démarrez la mise à niveau, les précontrôles de mise à niveau sont de nouveau exécutés et le nœud d'administration principal est automatiquement mis à niveau. Cette partie de la mise à niveau peut prendre jusqu'à 30 minutes.



Vous ne pourrez accéder à aucune autre page Grid Manager pendant la mise à niveau du nœud d'administration principal. Les journaux d'audit seront également indisponibles.

Étapes

1. Sélectionnez **Démarrer la mise à niveau**.

Un avertissement s'affiche pour vous rappeler que vous perdrez temporairement l'accès au Gestionnaire de grille.

2. Sélectionnez **OK** pour accuser réception de l'avertissement et démarrer la mise à niveau.
3. Attendez que les contrôles préalables de mise à niveau soient effectués et que le nœud d'administration principal soit mis à niveau.



Si des erreurs de vérification préalable sont signalées, résolvez-les et sélectionnez de nouveau **Démarrer la mise à niveau**.

Si la grille dispose d'un autre nœud d'administration en ligne et prêt, vous pouvez l'utiliser pour contrôler l'état du nœud d'administration principal. Dès que le nœud d'administration principal est mis à niveau, vous pouvez approuver les autres nœuds de la grille.

4. Si nécessaire, sélectionnez **Continuer** pour accéder à l'étape **mettre à niveau les autres nœuds**.

Mise à niveau des autres nœuds

Vous devez mettre à niveau tous les nœuds de la grille, mais vous pouvez effectuer plusieurs sessions de mise à niveau et personnaliser la séquence de mise à niveau. Par exemple, vous pouvez préférer mettre à niveau les nœuds sur le site A en une session, puis mettre à niveau les nœuds sur le site B dans une session ultérieure. Si vous choisissez d'effectuer la mise à niveau dans plusieurs sessions, sachez que vous ne pouvez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'ont pas été mis à niveau.

Si l'ordre de mise à niveau des nœuds est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le prochain nœud ou groupe de nœuds.



Lorsque la mise à niveau démarre sur un nœud de la grille, les services de ce nœud sont arrêtés. Plus tard, le nœud de la grille est redémarré. Pour éviter toute interruption de service pour les applications client qui communiquent avec le nœud, n'approuvez pas la mise à niveau d'un nœud, sauf si vous êtes sûr que le nœud est prêt à être arrêté et redémarré. Si nécessaire, planifiez une fenêtre de maintenance ou avisez les clients.

Étapes

1. Pour l'étape **mettre à niveau d'autres nœuds**, consultez le résumé, qui fournit l'heure de début de la mise à niveau dans son ensemble et l'état de chaque tâche de mise à niveau majeure.
 - **Démarrer le service de mise à niveau** est la première tâche de mise à niveau. Au cours de cette tâche, le fichier logiciel est distribué aux nœuds de grille et le service de mise à niveau est lancé sur chaque nœud.
 - 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, entrez 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 de package de récupération vous permet de restaurer le système en cas de panne.

3. Consultez les tableaux d'état pour chaque type de nœud. Il existe des tableaux pour les nœuds d'administration non primaires, les nœuds de passerelle et les nœuds de stockage.

Un nœud de grille peut se trouver dans l'une des étapes suivantes lorsque les tables apparaissent pour la première fois :

- Déballage de la mise à niveau
 - Téléchargement
 - En attente d'approbation
4. lorsque vous êtes prêt à sélectionner des nœuds de grille pour la mise à niveau (ou si vous devez annuler l'approbation des nœuds sélectionnés), utilisez les instructions suivantes :



Pour une mise à niveau de StorageGRID 12.1, si vous souhaitez approuver des nœuds individuels au lieu de tous les nœuds, la bonne pratique consiste à mettre à niveau un site entier avant de passer au site suivant.

Tâche	Instructions
Recherchez des nœuds spécifiques à approuver, tels que tous les nœuds d'un site particulier	Entrez la chaîne de recherche dans le champ Search
Sélectionnez tous les nœuds à mettre à niveau	Sélectionnez approuver tous les nœuds
Sélectionnez tous les nœuds du même type pour la mise à niveau (par exemple, tous les nœuds de stockage)	Sélectionnez le bouton Approve All pour le type de noeud Si vous approuvez plusieurs nœuds du même type, les nœuds seront mis à niveau un par un.
Sélectionnez un nœud individuel pour la mise à niveau	Sélectionnez le bouton Approve du nœud
Reporter la mise à niveau sur tous les nœuds sélectionnés	Sélectionnez Annuler l'approbation de tous les nœuds
Reporter la mise à niveau sur tous les nœuds sélectionnés du même type	Sélectionnez le bouton Annuler tout pour le type de noeud
Reporter la mise à niveau sur un nœud individuel	Sélectionnez le bouton Unapprove du nœud

5. Attendez que les nœuds approuvés passent par ces étapes de mise à niveau :
 - Approuvé et en attente de mise à niveau

- Arrêt des services



Vous ne pouvez pas supprimer un nœud lorsque sa scène atteint **Arrêt des services**. Le bouton **Unapprove** est désactivé.

- Arrêt du conteneur
- Nettoyage des images Docker
- Mise à niveau des packages OS de base



Lorsqu'un nœud d'appliance atteint ce stade, le logiciel StorageGRID Appliance installer de l'appliance est mis à jour. Ce processus automatisé garantit que la version du programme d'installation de l'appliance StorageGRID reste synchronisée avec la version du logiciel StorageGRID.

- Redémarrage



Certains modèles d'appliance peuvent redémarrer plusieurs fois pour mettre à niveau le micrologiciel et le BIOS.

- Exécution des étapes après le redémarrage
- Démarrage des services
- L'a fait

6. Répétez l' [étape d'approbation](#) autant de fois que nécessaire jusqu'à ce que tous les nœuds de grid aient été mis à niveau.

Mise à niveau terminée

Lorsque tous les nœuds de grille ont terminé les étapes de mise à niveau, la tâche **mettre à niveau d'autres nœuds de grille** s'affiche comme terminée. Les tâches de mise à niveau restantes sont effectuées automatiquement en arrière-plan.

Étapes

1. Dès que la tâche **Activer les fonctionnalités** est terminée (jusqu'à une heure), vous pouvez commencer à utiliser la ["nouvelles fonctionnalités"](#) dans la version mise à jour de StorageGRID.

Lorsque les **étapes finales de la mise à niveau** sont terminées, la mise à niveau est effectuée. La première étape, **Sélectionner les fichiers**, est réaffichée avec une bannière de succès verte.

2. Vérifiez que les opérations de la grille sont à nouveau normales :
 - a. Vérifiez que les services fonctionnent normalement et qu'il n'y a pas d'alerte inattendue.
 - b. Vérifiez que les connexions client au système StorageGRID fonctionnent comme prévu.

Informations associées

["Quel est l'impact de votre système pendant la mise à niveau"](#)

Résoudre les problèmes de mise à niveau de StorageGRID

Si un problème se produit lors de la mise à niveau, vous pouvez résoudre le problème vous-même. Si vous ne parvenez pas à résoudre un problème, collectez autant

d'informations que possible, puis contactez le support technique.

La mise à niveau n'est pas terminée

Les sections suivantes décrivent comment effectuer une restauration à partir de situations où la mise à niveau a partiellement échoué.

Erreurs de contrôle préalable de mise à niveau

Pour détecter et résoudre les problèmes, vous pouvez exécuter manuellement les contrôles préalables à la mise à niveau avant de démarrer la mise à niveau réelle. La plupart des erreurs de précontrôle fournissent des informations sur la façon de résoudre le problème.

Défaillances de provisionnement

Si le processus de provisionnement automatique échoue, contactez le support technique.

Le nœud de la grille tombe en panne ou ne parvient pas à démarrer

Si un nœud de la grille tombe en panne lors du processus de mise à niveau ou ne parvient pas à démarrer avec succès une fois la mise à niveau terminée, contactez le support technique pour rechercher et corriger les problèmes sous-jacents.

L'ingestion ou la récupération des données est interrompue

Si l'ingestion ou la récupération des données est interrompue de manière inattendue alors que vous ne mettez pas à niveau un nœud de grid, contactez le support technique.

Erreurs de mise à niveau de base de données

Si la mise à niveau de la base de données échoue avec une erreur, essayez à nouveau la mise à niveau. En cas d'échec à nouveau, contactez le support technique.

Informations associées

["Vérification de l'état du système avant la mise à niveau du logiciel"](#)

Problèmes liés à l'interface utilisateur

Vous pourriez rencontrer des problèmes avec le gestionnaire de grille ou le gestionnaire de locataires pendant ou après la mise à niveau.

Grid Manager affiche plusieurs messages d'erreur lors de la mise à niveau

Si vous actualisez votre navigateur ou accédez à une autre page Grid Manager pendant la mise à niveau du nœud d'administration principal, vous pouvez voir plusieurs messages « 503 : service indisponible » et « problème de connexion au serveur ». Vous pouvez ignorer ces messages en toute sécurité ; ils ne s'affichent plus dès que le nœud est mis à niveau.

Si ces messages s'affichent pendant plus d'une heure après le démarrage de la mise à niveau, il se peut que quelque chose ait empêché la mise à niveau du nœud d'administration principal. Si vous ne parvenez pas à résoudre le problème par vous-même, contactez le support technique.

L'interface Web ne répond pas comme prévu

Le gestionnaire de grid ou le gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

Si vous rencontrez des problèmes avec l'interface Web :

- Assurez-vous que vous utilisez un ["navigateur web pris en charge"](#).



La prise en charge des navigateurs a généralement été modifiée pour chaque version de StorageGRID.

- Effacez le cache de votre navigateur Web.

L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

Messages d'erreur « Docker image Availability check »

Lorsque vous tentez de démarrer le processus de mise à niveau, vous pouvez recevoir un message d'erreur indiquant que « les problèmes suivants ont été identifiés par la suite de validation de vérification de disponibilité d'image Docker ». Tous les problèmes doivent être résolus avant que vous puissiez terminer la mise à niveau.

Contactez le support technique si vous n'êtes pas certain des modifications requises pour résoudre les problèmes identifiés.

Messagerie	Cause	Solution
Impossible de déterminer la version de la mise à niveau. Le 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.	Téléchargez à nouveau le package de mise à niveau, puis réessayez. Si le problème persiste, contactez le support technique.
Le fichier d'informations sur la version de mise à niveau {file_path} est introuvable. Impossible de déterminer la version de la mise à niveau.	Le package de mise à niveau est corrompu.	Téléchargez à nouveau le package de mise à niveau, puis réessayez. Si le problème persiste, contactez le support technique.
Impossible de déterminer la version de la version actuellement installée sur {node_name}.	Un fichier critique du nœud est corrompu.	Contactez l'assistance technique.
Erreur de connexion lors de la tentative de liste des versions sur {node_name}	Le nœud est hors ligne ou la connexion a été interrompue.	Vérifiez que tous les nœuds sont en ligne et accessibles depuis le nœud d'administration principal, puis réessayez.

Messagerie	Cause	Solution
L'image StorageGRID n'est pas {upgrade_version} chargée sur l'hôte du nœud {node_name}. Les images et les services doivent être installés sur l'hôte avant que la mise à niveau ne puisse se poursuivre.	Les packages RPM ou DEB pour la mise à niveau n'ont pas été installés sur l'hôte sur lequel le nœud est en cours d'exécution, ou les images sont toujours en cours d'importation. Remarque : cette erreur s'applique uniquement aux nœuds qui s'exécutent en tant que conteneurs sous Linux.	Assurez-vous que les packages RPM ou DEB ont été installés sur tous les hôtes Linux sur lesquels des nœuds sont exécutés. Assurez-vous que la version est correcte pour le service et le fichier d'images. Attendez quelques minutes, puis réessayez. Voir " Linux : installez le package RPM ou DEB sur tous les hôtes ".
Erreur lors de la vérification du nœud {node_name}	Une erreur inattendue s'est produite.	Attendez quelques minutes, puis réessayez.
Erreur non détectée lors de l'exécution des contrôles préalables. {error_string}	Une erreur inattendue s'est produite.	Attendez quelques minutes, puis réessayez.

Appliquez le correctif StorageGRID

Procédure de correctif StorageGRID

Vous devrez peut-être appliquer un correctif à votre système StorageGRID si des problèmes liés au logiciel sont détectés et résolus entre les versions de fonctionnalités.

Les correctifs StorageGRID contiennent des modifications logicielles qui sont disponibles en dehors d'une version de fonctionnalité ou de correctif. Les mêmes modifications seront incluses dans une prochaine version. En outre, chaque version de correctif contient une synthèse de tous les correctifs précédents au sein de la fonction ou de la version de correctif.

Considérations relatives à l'application d'un correctif

Vous ne pouvez pas appliquer un correctif StorageGRID lorsqu'une autre procédure de maintenance est en cours d'exécution. Par exemple, vous ne pouvez pas appliquer un correctif lorsqu'une procédure de mise hors service, d'extension ou de récupération est en cours d'exécution.



Si une procédure de mise hors service d'un nœud ou d'un site est interrompue, vous pouvez appliquer un correctif en toute sécurité. De plus, vous pouvez appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau StorageGRID. Pour plus de détails, reportez-vous aux instructions de mise à niveau du logiciel StorageGRID.

Une fois le correctif téléchargé dans Grid Manager, le correctif est automatiquement appliqué au nœud d'administration principal. Vous pouvez ensuite approuver l'application du correctif sur les autres nœuds de votre système StorageGRID.

Si un correctif ne s'applique pas à un ou plusieurs nœuds, la raison de l'échec s'affiche dans la colonne Détails de la table de progression du correctif. Vous devez résoudre les problèmes qui ont causé les échecs, puis recommencer le processus tout entier. Les nœuds avec une application précédemment réussie du correctif

seront ignorés dans les applications suivantes. Vous pouvez réessayer en toute sécurité le processus de correctif autant de fois que nécessaire jusqu'à ce que tous les nœuds aient été mis à jour. Le correctif doit être installé avec succès sur tous les nœuds de la grille pour que l'application soit terminée.

Lorsque les nœuds de grille sont mis à jour avec la nouvelle version de correctif, les modifications réelles d'un correctif peuvent uniquement affecter des services spécifiques sur des types spécifiques de nœuds. Par exemple, un correctif peut uniquement affecter le service LDR sur les nœuds de stockage.

Application des correctifs pour la restauration et l'extension

Une fois un correctif appliqué à votre grille, le nœud d'administration principal ou un nœud d'administration secondaire installe automatiquement la même version du correctif sur tout nœud restauré par des opérations de récupération ou ajouté lors d'une extension. Vous pouvez récupérer n'importe quel nœud (y compris le nœud d'administration principal) lorsque vous êtes connecté à un nœud d'administration secondaire. Si vous récupérez un nœud à partir d'un nœud d'administration secondaire, ce nœud d'administration applique le correctif au nœud récupéré.

Si vous devez restaurer le nœud d'administration principal à partir de son propre programme d'installation StorageGRID, vous devez installer manuellement la version appropriée de StorageGRID, puis appliquer le correctif. La version finale de StorageGRID du nœud d'administration principal doit correspondre à celle des autres nœuds de la grille.

L'exemple suivant illustre comment appliquer un correctif lors de la récupération du nœud d'administration principal lorsque vous êtes connecté au nœud d'administration secondaire :

1. Supposons que la grille exécute une version StorageGRID 11.A.B avec le dernier correctif. La « version GRID » est 11.A.B.y.
2. Le nœud d'administration principal tombe en panne.
3. Vous redéployez le nœud d'administration principal à l'aide de StorageGRID 11.A.B et exécutez la procédure de restauration.



Si nécessaire pour correspondre à la version de grille, vous pouvez utiliser une version mineure lors du déploiement du nœud ; vous n'avez pas besoin de déployer la version majeure en premier.

4. Vous appliquez ensuite le correctif 11.A.B.y au nœud d'administration principal.

Comment StorageGRID est affecté lorsque vous appliquez un correctif

Vous devez comprendre comment votre système StorageGRID sera affecté lorsque vous appliquez un correctif.

Les correctifs StorageGRID ne perturbent pas l'activité

Le système StorageGRID peut ingérer et récupérer des données à partir des applications client tout au long du processus de correctif. Si vous approuvez tous les nœuds du même type au correctif (par exemple, nœuds de stockage), les nœuds sont arrêtés un par un, de sorte qu'il n'y a pas de temps lorsque tous les nœuds de grille ou tous les nœuds de grille d'un certain type sont indisponibles.

Pour assurer une disponibilité continue, vérifiez que votre règle ILM contient des règles qui spécifient le stockage de plusieurs copies de chaque objet. Vous devez également vous assurer que tous les clients S3 externes sont configurés pour envoyer des demandes à l'un des éléments suivants :

- Adresse IP virtuelle d'un groupe haute disponibilité (HA)
- Équilibreur de charge tiers haute disponibilité
- Plusieurs nœuds de passerelle pour chaque client
- Plusieurs nœuds de stockage pour chaque client

Les applications client peuvent subir des interruptions à court terme

Le système StorageGRID peut ingérer et récupérer les données des applications client tout au long du processus de correctif. Toutefois, les connexions client aux nœuds de passerelle ou de stockage individuels peuvent être interrompues temporairement si le correctif doit redémarrer les services sur ces nœuds. La connectivité sera restaurée une fois le processus de correctif terminé et les services reprendront sur les nœuds individuels.

Vous devrez peut-être planifier des temps d'arrêt pour appliquer un correctif si la perte de connectivité pendant une courte période n'est pas acceptable. Vous pouvez utiliser l'approbation sélective pour planifier la mise à jour de certains nœuds.



Vous pouvez utiliser plusieurs passerelles et groupes haute disponibilité (HA) pour assurer un basculement automatique pendant le processus de correctif. Voir les instructions pour ["configuration des groupes haute disponibilité"](#).

Des alertes et des notifications SNMP peuvent être déclenchées

Des alertes et des notifications SNMP peuvent être déclenchées lorsque les services sont redémarrés et lorsque le système StorageGRID fonctionne comme un environnement de version mixte (certains nœuds grid exécutant une version antérieure, alors que d'autres ont été mis à niveau vers une version ultérieure). En général, ces alertes et notifications seront claires lorsque le correctif sera terminé.

Les modifications de configuration sont restreintes

Lors de l'application d'un correctif à StorageGRID :

- N'apportez aucune modification à la configuration de la grille (par exemple, spécification de sous-réseaux Grid Network ou approbation de nœuds grid en attente) tant que le correctif n'a pas été appliqué à tous les nœuds.
- Ne mettez pas à jour la configuration ILM tant que le correctif n'a pas été appliqué à tous les nœuds.

Obtenez les matériaux nécessaires pour un correctif StorageGRID

Avant d'appliquer un correctif, vous devez obtenir tous les matériaux requis.

Élément	Remarques
Fichier de correctif StorageGRID	Vous devez télécharger le fichier de correctif StorageGRID.

Élément	Remarques
• Port réseau • "Navigateur Web pris en charge" • Client SSH (par exemple, PuTTY)	
Fichier de package de récupération (.zip)	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.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas répertoriée dans le Passwords.txt fichier.
Documentation associée	readme.txt pour le correctif. Ce fichier est inclus sur la page de téléchargement du correctif. Vérifiez soigneusement le readme fichier avant d'appliquer le correctif.

Télécharger un fichier correctif StorageGRID

Vous devez télécharger le fichier de correctif avant de pouvoir appliquer le correctif.

Étapes

1. Allez à "[Téléchargement NetApp : StorageGRID](#)".
2. Sélectionnez la flèche vers le bas sous **logiciel disponible** pour afficher la liste des correctifs disponibles au téléchargement.



Les versions de fichier correctif ont le format suivant : 11.4.x.y.

3. Vérifiez les modifications qui sont incluses dans la mise à jour.



Si vous avez juste "[Restauration du nœud d'administration principal - effectué](#)" et que vous devez appliquer un correctif, sélectionnez la même version de correctif installée sur les autres nœuds de grille.

- a. Sélectionnez la version du correctif que vous souhaitez télécharger et sélectionnez **Go**.
- b. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe de votre compte NetApp.
- c. Lisez et acceptez le contrat de licence de l'utilisateur final.

La page de téléchargement de la version sélectionnée s'affiche.

d. Téléchargez le fichier correctif `readme.txt` pour afficher un résumé des modifications incluses dans le correctif.

4. Sélectionnez le bouton de téléchargement du correctif et enregistrez le fichier.



Ne modifiez pas le nom de ce fichier.



Si vous utilisez un périphérique MacOS, il est possible que le fichier correctif soit automatiquement enregistré en tant que `.txt` fichier. Si c'est le cas, vous devez renommer le fichier sans l' `.txt` extension.

5. Sélectionnez un emplacement pour le téléchargement et sélectionnez **Enregistrer**.

Vérifiez l'état du système avant d'appliquer un correctif StorageGRID

Vous devez vérifier que le système est prêt à prendre en charge le correctif.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Si possible, assurez-vous que le système fonctionne normalement et que tous les nœuds de la grille sont connectés à la grille.

Les nœuds connectés ont des coches vertes  sur la page Nœuds.

3. Recherchez et résolvez les alertes en cours, si possible.
4. Assurez-vous qu'aucune autre procédure de maintenance n'est en cours, telle qu'une procédure de mise à niveau, de récupération, d'extension ou de mise hors service.

Vous devez attendre que toutes les procédures de maintenance actives soient terminées avant d'appliquer un correctif.

Vous ne pouvez pas appliquer un correctif StorageGRID lorsqu'une autre procédure de maintenance est en cours d'exécution. Par exemple, vous ne pouvez pas appliquer un correctif lorsqu'une procédure de mise hors service, d'extension ou de récupération est en cours d'exécution.



Si un nœud ou un site ["la procédure de mise hors service est suspendue"](#), vous pouvez appliquer un correctif en toute sécurité. De plus, vous pouvez appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau StorageGRID. Voir les instructions pour ["Mise à niveau du logiciel StorageGRID"](#).

Appliquer un correctif dans StorageGRID

Le correctif est d'abord appliqué automatiquement au nœud d'administration principal. Vous devez ensuite approuver l'application du correctif sur d'autres nœuds de la grille jusqu'à ce que tous les nœuds exécutent la même version logicielle. Vous pouvez personnaliser la séquence d'approbation en sélectionnant pour approuver des nœuds de grille individuels, des groupes de nœuds de grille ou tous les nœuds de la grille.

Avant de commencer

- Vous avez examiné le ["considérations relatives à l'application d'un correctif"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous disposez de l'accès racine ou de l'autorisation Maintenance.

Description de la tâche

- Vous pouvez retarder l'application d'un correctif à un nœud, mais le processus de correctif n'est pas terminé tant que vous n'avez pas appliqué le correctif à tous les nœuds.
- Vous ne pouvez pas effectuer de mise à niveau du logiciel StorageGRID ou de mise à jour du système d'exploitation SANtricity tant que vous n'avez pas terminé le processus de correctif.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Sélectionnez **Maintenance > Système > Mise à jour du logiciel**.

La page mise à jour du logiciel s'affiche.

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 correctif 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 correctif que vous avez téléchargé à partir du site de support NetApp.

- a. Sélectionnez **Parcourir**.
- b. Localisez et sélectionnez le fichier.

`hotfix-install-version`

- c. Sélectionnez **Ouvrir**.

Le fichier est téléchargé. Lorsque le téléchargement est terminé, le nom du fichier s'affiche dans le champ Détails.



Ne modifiez pas le nom du fichier car il fait partie du processus de vérification.

5. Entrez la phrase de passe de provisionnement dans la zone de texte.

Le bouton **Démarrer** devient activé.

6. Sélectionnez **Démarrer**.

Un avertissement s'affiche indiquant que la connexion de votre navigateur peut être perdue temporairement au fur et à mesure que les services sur le nœud d'administration principal sont redémarrés.

7. Sélectionnez **OK** pour commencer à appliquer le correctif au nœud d'administration principal.

Lorsque le correctif démarre :

- a. Les validations du correctif sont exécutées, y compris la vérification de la signature du code.



Si des erreurs sont signalées, résolvez-les, téléchargez à nouveau le fichier correctif et sélectionnez à nouveau **Démarrer**.

- b. Le tableau de progression de l'installation du correctif s'affiche.

Ce tableau affiche tous les nœuds de votre grille et l'étape actuelle de l'installation du correctif pour chaque nœud. Les nœuds du tableau sont regroupés par type (nœuds Admin, nœuds de passerelle et nœuds de stockage).

- c. La barre de progression atteint la fin, puis le nœud d'administration principal est affiché comme « terminé ».

Hotfix Installation Progress

Approve All Remove All

Admin Nodes - 1 out of 1 completed

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 en fonction de **site**, **Nom**, **progrès**, **étape** ou **Détails**. Vous pouvez également saisir un terme dans la zone **Rechercher** pour rechercher des nœuds spécifiques.
9. Approuver les nœuds grid prêts à être mis à jour. Les nœuds approuvés du même type sont mis à niveau un par un.



N'approuvez pas le correctif pour un nœud, sauf si vous êtes sûr que le nœud est prêt à être mis à jour. Lorsque le correctif est appliqué à un nœud de grille, certains services sur ce nœud peuvent être redémarrés. Ces opérations peuvent entraîner des interruptions de service pour les clients qui communiquent avec le nœud.

- Sélectionnez un ou plusieurs boutons **Approve** pour ajouter un ou plusieurs nœuds individuels à la file d'attente du correctif.
- Sélectionnez le bouton **approuver tout** dans chaque groupe pour ajouter tous les nœuds du même type à la file d'attente du correctif. Si vous avez saisi des critères de recherche dans la zone **recherche**, le bouton **approuver tout** s'applique à tous les nœuds sélectionnés par les critères de recherche.



Le bouton **approuver tout** en haut de la page approuve tous les nœuds répertoriés sur la page, tandis que le bouton **approuver tout** en haut d'un groupe de tables n'approuve que tous les nœuds de ce groupe. Si l'ordre dans lequel les nœuds sont mis à niveau est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le ou les nœuds suivants.

- Sélectionnez le bouton de niveau supérieur **approuver tout** en haut de la page pour ajouter tous les nœuds de la grille à la file d'attente du correctif.



Vous devez effectuer le correctif StorageGRID avant de lancer une autre mise à jour logicielle. Si vous ne parvenez pas à effectuer le correctif, contactez le support technique.

- Sélectionnez **Remove** ou **Remove All** pour supprimer un nœud ou tous les nœuds de la file d'attente du correctif.

Lorsque la phase progresse au-delà de « mise 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.

Lorsque le correctif a été correctement installé sur tous les nœuds, le tableau de progression de l'installation du correctif se ferme. Une bannière verte indique la date et l'heure de fin du correctif.

11. Si le correctif n'a pu être appliqué à aucun nœud, vérifiez l'erreur pour chaque nœud, résolvez le problème et répétez ces étapes.

La procédure n'est pas terminée tant que le correctif n'a pas été appliqué à tous les nœuds. Vous pouvez réessayer en toute sécurité le processus de correctif autant de fois que nécessaire jusqu'à ce qu'il soit terminé.

Configuration et gestion d'un système StorageGRID

Administrer StorageGRID

Démarrage rapide pour l'administration de StorageGRID

Suivez ces instructions pour configurer et administrer un système StorageGRID.



Assurez-vous d'avoir une compréhension générale du système StorageGRID et une connaissance assez détaillée des shells de commandes Linux, des réseaux et de la configuration matérielle des serveurs.

1

Commencez à utiliser Grid Manager

- ["Découvrez les étapes de base pour utiliser l'interface utilisateur de Grid Manager"](#)
- ["En savoir plus sur les informations relatives aux licences"](#)
- ["Découvrez comment utiliser l'API de gestion de grille"](#)

2

Contrôlez l'accès à StorageGRID

- ["Découvrez les phrases de passe, les mots de passe et les autorisations"](#)
- ["Configurer la fédération d'identité"](#)
- ["Gérez les groupes d'administration"](#)
- ["Gérer les utilisateurs"](#)
- ["Configurer l'authentification unique \(SSO\)"](#)

3

Utilisez la fédération de grilles

- ["Configurer les connexions de fédération de grille"](#)
- ["Découvrez la synchronisation des comptes"](#)
- ["Découvrez la réplication inter-grilles"](#)
- ["Configurer l'espace de noms global"](#)

4

Gérer la sécurité

- ["Étudiez les méthodes de cryptage StorageGRID"](#)
- ["Gérer les certificats"](#)
- ["Configurez les paramètres de sécurité"](#)
- ["Configurer les serveurs de gestion des clés"](#)
- ["Gérer les paramètres proxy"](#)

- "Contrôle des pare-feu"

5

Gérer les locataires

- "Découvrez et gérez les comptes locataires"
- "Gestion des services de plateforme pour les locataires"
- "Gérez S3 Select pour les comptes de locataires"

6

Configurer les connexions client

- "Découvrez la sécurité des clients S3"
- "Utilisez l'assistant d'installation S3"
- "Gérez les groupes haute disponibilité"
- "Configuration des noms de domaine de terminaux S3"

7

Gérer les réseaux et les connexions

- "Configurez les paramètres réseau"
- "Configurez les interfaces VLAN"
- "Gérer les stratégies de classification du trafic"
- "Gérer les coûts de liaison"

8

Gérer les nœuds

- "Gérer des nœuds de stockage"
- "Gérer les nœuds d'administration"

Lancez-vous avec Grid Manager

Configuration requise du navigateur Web pour StorageGRID

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Définissez la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Sign in au StorageGRID Grid Manager

Vous accédez à la page de connexion de Grid Manager en entrant le nom de domaine complet (FQDN) ou l'adresse IP d'un 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 primaires. Vous pouvez vous connecter au Gestionnaire de grille sur n'importe quel nœud d'administration pour gérer le système StorageGRID. Toutefois, certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Se connecter au groupe haute disponibilité

Si des nœuds admin sont inclus dans un groupe haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe haute disponibilité ou d'un nom de domaine complet mappé sur l'adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme interface principale du groupe, de sorte que lorsque vous accédez à Grid Manager, vous y accédez sur le nœud d'administration principal, sauf si le nœud d'administration principal n'est pas disponible. Voir ["Gérez les groupes haute disponibilité"](#).

Utiliser SSO

Les étapes de connexion sont légèrement différentes si ["L'authentification unique \(SSO\) a été configurée"](#).

Connectez-vous à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous utilisez un ["navigateur web pris en charge"](#).
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs disposant d'au moins une autorisation.
- Vous avez l'URL du Gestionnaire de grille :

```
https://FQDN_or_Admin_Node_IP/
```

Vous pouvez utiliser le nom de domaine complet, l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration.

Pour accéder au Gestionnaire de grille sur un port autre que le port par défaut pour HTTPS (443), indiquez le numéro de port dans l'URL :

```
https://FQDN_or_Admin_Node_IP:port/
```

Étapes

1. Lancez un navigateur Web pris en charge.

2. Dans la barre d'adresse du navigateur, entrez l'URL du Gestionnaire de grille.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur. Voir "[Gérer les certificats de sécurité](#)".
4. Connectez-vous au Grid Manager.

L'écran de connexion qui s'affiche dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

Pas d'utilisation de SSO

- a. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
- b. Sélectionnez **connexion**.

Utilisation de SSO

- Si StorageGRID utilise SSO pour la première fois que vous accédez à l'URL de ce navigateur :
 - i. Sélectionnez **connexion**. Vous pouvez laisser le 0 dans le champ compte.
 - ii. Saisissez vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation.

Par exemple, si StorageGRID utilise SSO et que vous avez déjà accédé au Grid Manager ou à un compte de locataire :

- A. Entrez **0** (l'ID de compte du gestionnaire de grille) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.
- B. Sélectionnez **connexion**.
- C. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Lorsque vous êtes connecté, la page d'accueil du Gestionnaire de grille s'affiche, qui inclut le tableau de bord. Pour savoir quelles informations sont fournies, reportez-vous "[Affichez et gérez le tableau de bord](#)" à la section .

Connectez-vous à un autre nœud d'administration

Procédez comme suit pour vous connecter à un autre nœud d'administration.

Pas d'utilisation de SSO

Étapes

1. Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Indiquez le numéro de port requis.
2. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
3. Sélectionnez **connexion**.

Utilisation de SSO

Si StorageGRID utilise SSO et que vous vous êtes connecté à un nœud d'administration, vous pouvez accéder à d'autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

1. Entrez le nom de domaine complet ou l'adresse IP de l'autre 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 StorageGRID Grid Manager

Lorsque vous avez terminé de travailler avec le Gestionnaire de grille, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Sélectionnez votre nom d'utilisateur dans le coin supérieur droit.
2. Sélectionnez **Déconnexion**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. Remarque : si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédez. La page de connexion StorageGRID s'affiche. Grid Manager est répertorié comme valeur par défaut dans la liste déroulante comptes récents et le champ ID compte affiche 0. Remarque : si l'authentification unique est activée et que vous êtes également connecté au gestionnaire de locataires, vous devez également "déconnectez-vous du compte du locataire" à "Déconnectez-vous de SSO" .

Modifiez votre mot de passe StorageGRID Grid Manager

Si vous êtes un utilisateur local de Grid Manager, vous pouvez modifier votre propre mot de passe.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans le Gestionnaire de grille. Vous devez plutôt modifier votre mot de passe dans le référentiel d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez **votre nom** > **changer mot de passe**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

Votre mot de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les mots de passe sont sensibles à la casse.

4. Saisissez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Afficher les informations de licence StorageGRID

Vous pouvez afficher les informations relatives aux licences de votre système StorageGRID, comme la capacité de stockage maximale de votre réseau, si nécessaire.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

En cas de problème avec la licence logicielle de ce système StorageGRID, la carte d'état d'intégrité du tableau de bord comprend une icône d'état de la licence et un lien **Licence**. Ce numéro indique le nombre de problèmes liés à la licence.



Étapes

1. Accédez à la page Licence en effectuant l'une des opérations suivantes :
 - Sélectionnez **Maintenance > Système > Licence**.
 - Dans la carte d'état d'intégrité du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**.

Ce lien apparaît uniquement en cas de problème avec la licence.

2. Afficher les détails en lecture seule de la licence actuelle :
 - ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
 - Numéro de série de la licence
 - Type de licence, soit **perpétuel** soit **abonnement**
 - Capacité de stockage sous licence de la grille
 - Capacité de stockage prise en charge
 - Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
 - Date de fin du support

Cette date est extraite du fichier de licence actuel et peut être obsolète si vous avez prolongé ou renouvelé le contrat de service d'assistance après l'obtention du fichier de licence. Pour mettre à jour cette valeur, consultez "[Mettez à jour les informations de licence StorageGRID](#)". Vous pouvez également consulter la date de fin de contrat réelle à l'aide de Digital Advisor.

- Contenu du fichier texte de licence

Mettez à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID à tout moment que les conditions de votre modification de licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez de la capacité de stockage supplémentaire pour votre grid.

Avant de commencer

- Vous avez un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez la phrase secrète pour le 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 pour le provisionnement.
5. Sélectionnez **Enregistrer**.

Utilisez l'API

Utilisez l'API de gestion de grille StorageGRID

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management plutôt que de l'interface utilisateur Grid Manager. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

Ressources générales

L'API de gestion du grid fournit les ressources de premier niveau suivantes :

- `/grid`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées.
- `/org`: L'accès est limité aux utilisateurs qui appartiennent à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, voir ["Utilisez un compte de locataire"](#).
- `/private`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API Grid Management utilise la plateforme d'API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).



Toutes les opérations d'API que vous effectuez à l'aide de la page Web Documentation de l'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. Dans l'en-tête de Grid Manager, sélectionnez l'icône d'aide  et sélectionnez **Documentation API**.
2. Pour effectuer une opération avec l'API privée, sélectionnez **accéder à la documentation API privée** sur la page API de gestion StorageGRID.

Les API privées sont susceptibles d'être modifiées sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

3. Sélectionnez l'opération souhaitée.

Lorsque vous développez une opération API, vous pouvez voir les actions HTTP disponibles, telles QUE GET, PUT, UPDATE ou DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, notamment l'URL du noeud final, la

liste de tous les paramètres obligatoires ou facultatifs, un exemple de l'organisme de demande (si nécessaire) et les réponses possibles.

groups Operations on groups

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 typeapplication/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, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
- Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.
- Sélectionnez **essayez-le**.
- Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
- Sélectionnez **Exécuter**.

10. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Opérations de l'API de gestion de la grille dans StorageGRID

L'API Grid Management organise les opérations disponibles dans les sections suivantes.



Cette liste inclut uniquement les opérations disponibles dans l'API publique.

- **Comptes** : opérations de gestion des comptes de locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **Alert-history** : opérations sur les alertes résolues.
- **Alerteurs** : opérations sur les récepteurs de notification d'alerte (e-mail).
- **Alert-rules** : opérations sur les règles d'alerte.
- **Silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : opérations sur les alertes.
- **Audit** : opérations pour répertorier et mettre à jour la configuration de l'audit.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

L'API Grid Management prend en charge le schéma d'authentification par jeton Bearer. Pour vous connecter, vous devez fournir un nom d'utilisateur et un mot de passe dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : porteur *token* »). Le jeton expire au bout de 16 heures.



Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Reportez-vous à la section « authentification dans l'API si l'authentification unique est activée ».

Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, reportez-vous à la section « protection contre la falsification de demandes intersites ».

- **Certificats-client** : opérations permettant de configurer les certificats client afin que StorageGRID soit accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **Config** : opérations liées à la version du produit et aux versions de l'API Grid Management. Vous pouvez répertorier la version du produit et les principales versions de l'API Grid Management prises en charge par cette version, et désactiver les versions obsolètes de l'API.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **dns-servers** : opérations permettant de répertorier et de modifier les serveurs DNS externes configurés.
- **Drive-details** : Opérations sur les lecteurs pour des modèles de dispositifs de stockage spécifiques.
- **Endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine des noeuds finaux S3.
- **Code d'effacement** : opérations sur les profils de code d'effacement.
- **Expansion** : opérations d'expansion (au niveau de la procédure).
- **Noeuds-expansion** : Opérations sur expansion (niveau noeud).
- **Sites d'expansion** : opérations d'expansion (au niveau du site).

- **GRID-Networks** : opérations permettant de répertorier et de modifier la liste des réseaux de la grille.
- **GRID-mots de passe** : opérations pour la gestion des mots de passe de la grille.
- **Groupes** : opérations permettant de gérer les groupes d'administrateurs de grille locaux et de récupérer les groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **ilm** : opérations sur la gestion du cycle de vie de l'information (ILM).
- **Procédures en cours** : récupère les procédures de maintenance en cours.
- **License** : opérations de récupération et de mise à jour de la licence StorageGRID.
- **Logs** : opérations de collecte et de téléchargement des fichiers journaux.v
- **Metrics** : opérations sur les métriques StorageGRID, y compris les requêtes métriques instantanées à un point dans le temps et les requêtes métriques de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.



Les mesures qui incluent *private* dans leur nom sont destinées à un usage interne uniquement. Ces metrics sont susceptibles d'être modifiés sans préavis entre les versions d'StorageGRID.

- **Node-details** : opérations sur les détails de noeud.
- **Node-Health** : opérations sur l'état d'intégrité du nœud.
- **État-stockage-noeud** : opérations sur l'état de stockage du noeud.
- **nntp-servers** : opérations de liste ou de mise à jour des serveurs NTP (Network Time Protocol) externes.
- **Objets** : opérations sur les objets et les métadonnées des objets.
- **Récupération** : opérations pour la procédure de récupération.
- **recovery-package** : Opérations de téléchargement du package de récupération.
- **Régions** : opérations pour afficher et créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-certificate** : opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **Filigranes de stockage** : filigranes de nœuds de stockage.
- **Classes de trafic** : opérations pour les politiques de classification du trafic.
- **Ingest-client-network** : opérations sur la configuration réseau client non fiable.
- **Utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API Grid Management dans StorageGRID

L'API de gestion du grid utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version majeure de l'API est incrémentée lorsque des modifications sont effectuées qui ne sont *pas compatibles* avec des versions plus anciennes. La version mineure de l'API est incrémentée lorsque des modifications qui sont *compatibles* avec des versions plus anciennes sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2,1	2,2
Non compatible avec les versions plus anciennes	2,1	3,0

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 StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.



Vous pouvez configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section **config** de la documentation de l'API swagger "[API de gestion du grid](#)". Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la nouvelle version.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la GET `/versions` requête API pour renvoyer une liste des versions majeures de l'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
  ]
}
```

Spécifiez une version API pour une demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (/api/v4) ou d'un en-tête (Api-Version: 4). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protégez-vous contre les attaques Cross-Site Request Forgery (CSRF) dans StorageGRID

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez le `csrfToken` paramètre sur `true` pendant l'authentification. La valeur par défaut est `false`.


```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Lorsque la valeur est true, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- L'`X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé en forme : un `csrfToken` paramètre de corps de requête codé en forme.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.



Les demandes qui ont un ensemble de cookies de token CSRF appliquent également l'en-tête « Content-Type: Application/json » pour toute demande qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée

Utilisez l'API StorageGRID si l'authentification unique est activée (Active Directory)

Si vous avez "[Authentification unique \(SSO\) configurée et activée](#)" 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.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

- Un exemple de flux de travail des requêtes Curl.

Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. Vous pouvez voir l'erreur : `A valid SubjectConfirmation was not found on this Response.`



L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, vous pouvez 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.
 - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez-le à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

- Méthode SSO. Entrez ADFS ou adfs.
- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé
- L'adresse de StorageGRID
- L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.
 - a. Déclarez les variables nécessaires pour la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

- b. Pour recevoir une URL d'authentification signée, envoyez une demande POST à `/api/v3/authorize-saml` et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à `python -m json.tool` pour supprimer le codage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H "Content-Type: application/json" \
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
  sSl%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Enregistrez la SAMLRequest à partir de la réponse pour l'utiliser dans les commandes suivantes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Obtenir une URL complète incluant l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion à l'aide de l'URL de la réponse précédente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La réponse inclut l'ID de demande client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRTomwFIZfzhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Enregistrez l'ID de la demande client à partir de la réponse.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envoyez vos informations d'identification à l'action de formulaire de la réponse précédente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$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 post du formulaire contiendra également le deuxième mot de passe ou d'autres informations d'identification.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=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
```

g. Enregistrez le `MSISAuth` cookie de la réponse.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envoyez une demande GET à l'emplacement spécifié avec les cookies du POST d'authentification.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Les en-têtes de réponse contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse dans un champ de formulaire masqué.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeSlBZGlpbi0xNzgmrMfsc2Umcng4NnJDZmFKV
XFXVWx3bkllMnFuUSUZZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDkzMjc0Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjoloVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbwXwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Enregistrer le SAMLResponse à partir du champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. A l'aide de la commande enregistrée SAMLResponse, faites une demande StorageGRID/api/saml-response pour générer un jeton d'authentification StorageGRID.

Pour RelayState, utilisez l'ID de compte de locataire ou utilisez 0 si vous souhaitez vous connecter à l'API de gestion de grille.

```
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, comme vous le feriez pour utiliser l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, 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 redirection vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Supprimez le jeton de support StorageGRID.

La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" 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
```

Une 204 No Content réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Utilisez l'API StorageGRID si l'authentification unique est activée (Entra ID)

Si vous avez "[Authentification unique \(SSO\) configurée et activée](#)" et vous utilisez Entra ID 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 Entra ID est activée

Ces instructions s'appliquent si vous utilisez Entra ID comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez l'adresse e-mail SSO et le mot de passe d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` script Python
- `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour écrire votre propre intégration API avec Entra ID, 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 Entra ID 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 SSO Entra ID.

Si vous avez un problème de codage d'URL, vous pouvez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Installez les dépendances requises comme suit :

- a. Installez Node.js (voir "<https://nodejs.org/en/download/>").
- b. Installez les modules Node.js requis (maripeteer et jsdom) :

```
npm install -g <module>
```

2. Passez le script Python à l'interpréteur Python pour exécuter le script.

Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions SSO Entra ID.

3. Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
 - L'adresse e-mail SSO utilisée pour se connecter à Entra ID
 - L'adresse de StorageGRID
 - L'ID du compte de locataire, pour accéder à l'API de gestion des locataires
4. Lorsque vous y êtes invité, saisissez le mot de passe et soyez prêt à fournir une autorisation MFA à Entra ID si demandé.

```
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 l'authentificateur Microsoft. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes de MFA (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

Utilisez l'API StorageGRID si l'authentification unique est activée (PingFederate)

Si vous avez "[Authentification unique \(SSO\) configurée et activée](#)" 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.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail des requêtes Curl.

Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. Vous pouvez voir l'erreur : `A valid SubjectConfirmation was not found on this Response.`



L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, vous pouvez 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.
 - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez-le à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

- Méthode SSO. Vous pouvez entrer n'importe quelle variation de "pingfederate" (PINGFEDERATE, pingfederate, et ainsi de suite).
- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou entrer n'importe quelle valeur.
- L'adresse de StorageGRID
- L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

- a. Déclarez les variables nécessaires pour la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

- b. Pour recevoir une URL d'authentification signée, envoyez une demande POST à /api/v3/authorize-saml et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool pour supprimer l'encodage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H "Content-Type: application/json" \
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Enregistrez la SAMLRequest à partir de la réponse pour l'utiliser dans les commandes suivantes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Exportez la réponse et le cookie, et écho la réponse :

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporter la valeur 'pf.adapterId' et réafficher la réponse :

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporter la valeur « href » (supprimer la barre oblique inverse /) et afficher en écho la réponse :

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporter la valeur « action » :

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Envoyer des cookies avec des informations d'identification :

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Enregistrer le SAMLResponse à partir du champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. A l'aide de la commande enregistré SAMLResponse, faites une demande StorageGRID/api/saml-response pour générer un jeton d'authentification StorageGRID.

Pour RelayState, utilisez l'ID de compte de locataire ou utilisez 0 si vous souhaitez vous connecter à l'API de gestion de grille.

```
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, comme vous le feriez pour utiliser l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, 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 redirection vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Supprimez le jeton de support StorageGRID.

La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si le 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
```

Une 204 No Content réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Désactivez les fonctionnalités de StorageGRID avec l'API

Vous pouvez utiliser l'API de gestion de grille pour désactiver complètement certaines fonctions du système StorageGRID. Lorsqu'une fonction est désactivée, aucune autorisation ne peut être attribuée pour effectuer les tâches associées à cette fonctionnalité.

Description de la tâche

Le système de fonctions désactivées vous permet d'empêcher l'accès à certaines fonctions du système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur racine ou les utilisateurs appartenant à des groupes d'administration disposant de l'autorisation **accès racine** d'utiliser cette fonctionnalité.

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte le scénario suivant :

La Société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

*Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de grille. En désactivant complètement la fonction **Modifier le mot de passe root** du locataire dans le Gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A garantit que les utilisateurs Admin, y compris l'utilisateur root et les utilisateurs appartenant à des groupes avec l'autorisation **Root Access**, ne peuvent pas modifier le mot de passe de l'utilisateur root d'un compte de locataire.*

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management. Voir "[Utilisez l'API de gestion du grid](#)".
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour désactiver une fonction, par exemple changer le mot de passe racine du locataire, envoyez un corps à l'API comme suit :

```
{ "grid": {"changeTenantRootPassword": true} }
```

Une fois la demande terminée, la fonction de modification du mot de passe racine du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe root** du locataire n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe root d'un locataire échoue avec "403 interdit".

Réactiver les fonctions désactivées

Par défaut, vous pouvez utiliser l'API Grid Management pour réactiver une fonction qui a été désactivée. Toutefois, si vous souhaitez empêcher la réactivation des fonctions désactivées, vous pouvez désactiver la fonction **activeFeatures** elle-même.



La fonction **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonction, sachez que vous perdrez définitivement la capacité de réactiver les autres fonctions désactivées. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management.
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

```
{ "grid": null }
```

Lorsque cette demande est terminée, toutes les fonctions, y compris la fonction Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine** du locataire apparaît maintenant dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire va réussir, en supposant que l'utilisateur dispose de l'autorisation de gestion **accès racine** ou **changer le mot de passe racine du locataire**.



L'exemple précédent provoque la réactivation des fonctions **ALL DESACTIVE**. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe root du locataire et continuer à désactiver l'autorisation de gestion storageAdmin, envoyez cette demande PUT:

```
{ "grid": {"storageAdmin": true} }
```

Contrôle de l'accès à StorageGRID

Contrôlez l'accès au 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, puis en attribuant des permissions à chaque groupe. Vous pouvez également activer l'authentification unique (SSO), créer des certificats clients, modifier les mots de passe de la grille et utiliser la vérification multi-administrateurs.

Contrôle de l'accès au Grid Manager

Vous déterminez qui peut accéder à Grid Manager et à l'API Grid Management en important des groupes et des utilisateurs à partir d'un service de fédération des identités ou en configurant des groupes locaux et des utilisateurs locaux.

L'utilisation de "[fédération des identités](#)" rend la configuration "[groupes](#)" et "[utilisateurs](#)" plus rapide, et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification habituelles. Vous pouvez configurer la fédération des identités si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.



Contactez le support technique si vous souhaitez utiliser un autre service LDAP v3.

Vous déterminez les tâches que chaque utilisateur peut effectuer en affectant différentes tâches "[autorisations](#)" à chaque groupe. Par exemple, il peut être nécessaire que les utilisateurs d'un groupe puissent gérer les règles ILM et les utilisateurs d'un autre groupe pour effectuer les tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

Vous pouvez également configurer un groupe pour qu'il soit en lecture seule. Les utilisateurs d'un groupe en lecture seule peuvent uniquement afficher les paramètres et les fonctions. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou Grid Management.

Activez l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de Security Assertion Markup Language 2.0 (SAML 2.0) ou de la norme OpenID Connect (OIDC). Après que vous "[Configurez et activez 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 de gestion du Grid ou à l'API de gestion du Tenant. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifiez la phrase secrète du provisionnement

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 "[modifiez la phrase de passe](#)" selon les besoins.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud, 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 "[modifiez le mot de passe de la console du nœud](#)" pour chaque nœud.

Utilisez la vérification multi-administrateurs

Vous pouvez utiliser la vérification multi-administrateurs (MAV) pour garantir que certaines opérations StorageGRID ne puissent être effectuées qu'après approbation des administrateurs désignés. La MAV empêche les administrateurs compromis, malveillants ou inexpérimentés d'apporter des modifications indésirables ou de supprimer des données.

Modifier la phrase secrète de provisionnement StorageGRID

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 Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

La phrase secrète de provisionnement est requise pour 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 grille**.
2. Sous **Modifier la phrase de passe de provisionnement**, sélectionnez **faire une modification**

3. Saisissez votre phrase secrète pour le provisionnement.
4. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases passe sont sensibles à la casse.



Stockez la phrase secrète de provisionnement dans un endroit sûr. Il est nécessaire pour les procédures d'installation, d'extension et de maintenance.

5. Saisissez à nouveau la nouvelle phrase de passe et sélectionnez **Enregistrer**.

Le système affiche une bannière verte de réussite lorsque la modification de la phrase de passe de provisionnement est terminée.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Sélectionnez **progiciel de récupération**.
7. 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 de package de récupération vous permet de restaurer le système en cas de panne.

Modifier les mots de passe des consoles de nœud dans StorageGRID

Chaque nœud de votre grille dispose d'un mot de passe de console de nœud, que vous utilisez pour vous connecter au nœud. Par défaut, chaque nœud possède un mot de passe unique. Vous pouvez modifier chaque mot de passe par un nouveau mot de passe unique ou modifier le mot de passe de chaque nœud pour utiliser un mot de passe global. Les mots de passe sont stockés dans le package de récupération.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

Vous utilisez un mot de passe de console de 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. Vous pouvez modifier les mots de passe de la console du nœud à l'aide de l'une de ces options :

- Appliquer automatiquement des mots de passe aléatoires à chaque nœud
- Spécifiez et appliquez un mot de passe global à tous les nœuds
- Spécifiez et appliquez un mot de passe unique à un ou plusieurs nœuds

Les mots de passe sont stockés 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.



Le "**Mots de passe d'accès SSH**" car les clés SSH utilisées pour la communication entre les nœuds sont distinctes des mots de passe de la console des nœuds. Cette procédure ne modifie pas les mots de passe d'accès SSH.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Mots de passe de grille**.
2. Sous **Modifier les mots de passe de la console de nœuds**, sélectionnez **faire une modification**.

Téléchargez 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. Saisissez la phrase de passe de provisionnement pour votre grid.
2. Sélectionnez **Télécharger le paquet 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 du système StorageGRID .

4. Sélectionnez **Continuer**.

Fournir de nouveaux mots de passe

1. Sélectionnez la méthode de changement de mot de passe que vous souhaitez utiliser.
 - **Automatique** : StorageGRID attribue automatiquement un nouveau mot de passe de console aléatoire à tous les nœuds.
 - **Personnalisé** : Vous fournissez les mots de passe de la console.

Automatique

1. Sélectionnez **Continuer**.

Personnalisées

1. Sélectionnez l'une des options suivantes :
 - **Mot de passe de la console globale** : appliquez le même mot de passe de console à tous les nœuds.
 - **Mots de passe de console uniques** : appliquez un mot de passe différent sur un ou plusieurs nœuds.
2. Si vous avez sélectionné **Mot de passe de la console globale**, saisissez le mot de passe que vous souhaitez utiliser pour tous les nœuds.
3. Si vous avez sélectionné **Mots de passe de console uniques**, saisissez un mot de passe unique pour un ou plusieurs nœuds.
4. Sélectionnez **Continuer**.

Terminer le changement de mot de passe

1. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** si vous êtes prêt à ce que StorageGRID commence à modifier les mots de passe de la console du nœud.



Vous ne pouvez pas annuler ce processus après son démarrage.

StorageGRID génère un nouveau package de récupération contenant le nouveau mot de passe.

2. Lorsque le nouveau package de récupération est prêt, sélectionnez **Télécharger le nouveau package de récupération** et enregistrez le package de récupération.
3. Ouvrez le `.zip` fichier.
4. Vérifiez que vous pouvez accéder au contenu, y compris au `Passwords.txt` fichier qui contient les nouveaux mots de passe de la console du nœud.
5. Copiez le nouveau fichier de package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.



N'écrasez pas l'ancien package de récupération.

Vous devez sécuriser le fichier de récupération, 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 pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
7. Sélectionnez **Continuer**.

StorageGRID met à jour le mot de passe pour chaque nœud.

S'il y a une erreur pendant le processus de mise à jour, la barre de progression indique 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.

8. Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :
 - a. Vérifiez les messages d'erreur répertoriés dans le tableau.
 - b. Résolvez les problèmes.
 - c. Sélectionnez **Réessayer**.



La tentative de nouveau modifie uniquement les mots de passe de la console de nœud sur les nœuds qui ont échoué lors des précédentes tentatives de changement de mot de passe.

9. Lorsque la barre de progression indique qu'il ne reste aucune mise à jour, sélectionnez **Terminer**.
10. 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](#).

Modifier les mots de passe d'accès SSH pour les nœuds d'administration StorageGRID

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 via une authentification sécurisée 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 VM ou une connexion à une console physique.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la 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. Celles-ci ne sont pas modifiées par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Mots de passe de grille**.
2. Sous **Modifier les clés SSH**, sélectionnez **faire une modification**.

Téléchargez 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 de passe de provisionnement pour votre grid.

2. Sélectionnez **Télécharger le paquet 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 du système StorageGRID .

4. Sélectionnez **Continuer**.
5. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** si vous êtes prêt à changer les clés d'accès SSH.



Vous ne pouvez pas annuler ce processus après son démarrage.

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 fichier.
 - b. Vérifiez que vous pouvez accéder au contenu, y compris au Passwords.txt fichier qui contient les nouvelles clés d'accès SSH.
 - c. Copiez le nouveau fichier de 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 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 s'affiche.

En cas d'erreur lors du processus de mise à jour, un message d'avertissement indique 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 pu être modifiée. Si le processus se termine alors que certains nœuds n'ont toujours pas de clé modifiée, le bouton **Réessayer** s'affiche.

Si la mise à jour de la clé a échoué pour un ou plusieurs nœuds :

- a. Vérifiez les messages d'erreur répertoriés dans le tableau.
- b. Résolvez les problèmes.

c. Sélectionnez **Réessayer**.

La reconnexion ne modifie que les clés d'accès SSH sur les nœuds qui ont échoué lors des tentatives précédentes de changement de clé.

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 > Package de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Utilisez la fédération d'identité dans StorageGRID

L'utilisation de la fédération des identités accélère la configuration des groupes et des utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification familières.

Configurer la fédération des identités pour Grid Manager

Vous pouvez configurer la fédération 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, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#) .
- Vous avez ["autorisations d'accès spécifiques"](#) .
- Vous utilisez Active Directory, Microsoft Entra ID, 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 avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Instructions de configuration d'un serveur OpenLDAP](#).
- Si vous envisagez d'activer l'authentification unique (SSO), vous avez examiné le ["configuration requise et considérations pour l'authentification unique"](#) .
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identités utilise TLS 1.2 ou 1.3. Voir ["Chiffrement pris en charge pour les connexions TLS sortantes"](#).

Description de la tâche

Vous pouvez configurer une source d'identité pour Grid Manager si vous souhaitez importer des groupes à partir d'un autre système tel qu'Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administration. Les utilisateurs des groupes admin peuvent se connecter au gestionnaire de grille et effectuer des tâches en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre référentiel d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Gestionnaire de locataires et effectuer des tâches en fonction des autorisations attribuées au groupe dans le Gestionnaire de locataires. Voir ["Créer un compte de locataire"](#) et ["Utilisez un compte de locataire"](#) pour plus de détails.

Entrez la configuration

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
 - **Nom unique 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, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
 - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
 - **Port** : port utilisé pour se connecter au serveur LDAP.



Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur

LDAP.

Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- sAMAccountName ou uid
 - objectGUID, entryUUID ou nsuniqueid
 - cn
 - memberOf ou isMemberOf
 - **Active Directory** : objectSid, primaryGroupID, userAccountControl et userPrincipalName
 - **Entra ID**: accountEnabled et userPrincipalName
- **Mot de passe** : 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 de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.



Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

- **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

- **Modèle UserPrincipalName (AD et Entra ID)**: [USERNAME]@example.com
- **Modèle de nom de connexion de niveau inférieur (AD et Entra ID)**: example\[USERNAME]
- **Motif de nom distinctif** : CN=[USERNAME],CN=Users,DC=example,DC=com

Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

- **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 Microsoft Entra ID.
- **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Microsoft Entra ID.
- **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 Microsoft Entra ID.



L'utilisation de l'option **Ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
 - Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s'affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Si les paramètres de connexion ne sont pas valides, le message « Impossible d'établir la connexion de test » s'affiche. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.

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](#)

- Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s’affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d’erreur s’affiche si les paramètres de connexion, le format du nom d’utilisateur de liaison ou le nom d’utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d’identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d’identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.



L’alerte **échec de synchronisation de la fédération d’identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d’identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération 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.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l’accès au système StorageGRID

jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.

- La synchronisation entre le système StorageGRID et la source d'identité ne se produira pas 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'état de l'authentification unique (SSO) est **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 des identités.
2. Décochez la case **Activer la fédération d'identité**.

Instructions de configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les sources d'identité qui ne sont pas Active Directory ou Microsoft Entra ID, 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.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance des membres de groupe inversé dans le ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"](#).

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations sur la maintenance de l'appartenance à ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"](#)un groupe inversé dans le .

Informations associées

["Ports utilisés pour les communications externes"](#)

Gérer les groupes d'administrateurs dans StorageGRID

Vous pouvez créer des groupes d'administration pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un

groupe pour pouvoir accéder au système StorageGRID.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Créer un groupe d'administration

Les groupes Admin vous permettent de déterminer quels utilisateurs peuvent accéder aux fonctions et opérations du gestionnaire de grille et de l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Groupes d'administrateurs**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs à partir du référentiel d'identité.

Groupe local

Étapes

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d'affichage pour le groupe, que vous pourrez mettre à jour ultérieurement si nécessaire. Par exemple, « utilisateurs de maintenance » ou « administrateurs ILM ».
3. Entrez un nom unique pour le groupe que vous ne pourrez pas mettre à jour ultérieurement.
4. Sélectionnez **Continuer**.

Groupe fédéré

Étapes

1. Sélectionnez **Groupe fédéré**.
2. Entrez le nom du groupe à importer, exactement tel qu'il apparaît dans le référentiel d'identité configuré.
 - Pour Active Directory et Microsoft Entra ID, utilisez sAMAccountName.
 - Pour OpenLDAP, utilisez le CN (Common Name).
 - Pour un autre LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Étapes

1. Pour **mode d'accès**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans le gestionnaire de grille et l'API de gestion de grille ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités.
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
 - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou Grid Management. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs "[autorisations de groupe d'administration](#)".

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant au groupe ne pourront pas se connecter à StorageGRID.

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter ce groupe à l'utilisateur sur la page utilisateurs. Voir "[Gérer les utilisateurs](#)" pour plus de détails.

2. Sélectionnez **Créer groupe** et **Terminer**.

Afficher et modifier les groupes d'administration

Vous pouvez afficher les détails des groupes existants, modifier un groupe ou dupliquer un groupe.

- Pour afficher les informations de base de tous les groupes, consultez le tableau de la page groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **actions** ou la page de détails.

Tâche	Menu actions	Page de détails
Afficher les détails du groupe	a. Cochez la case du groupe. b. Sélectionnez actions > Afficher les détails du groupe .	Sélectionnez le nom du groupe dans le tableau.

Tâche	Menu actions	Page de détails
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case du groupe. b. Sélectionnez actions > Modifier le nom du groupe . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône de modification  . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications .
Modifier le mode d'accès ou les autorisations	a. Cochez la case du groupe. b. Sélectionnez actions > Afficher les détails du groupe . c. Si vous le souhaitez, modifiez le mode d'accès du groupe. d. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration" . e. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Si vous le souhaitez, modifiez le mode d'accès du groupe. c. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration" . d. Sélectionnez Enregistrer les modifications .

Dupliquer un groupe

Étapes

1. Cochez la case du groupe.
2. Sélectionnez **actions > Dupliquer le groupe**.
3. Suivez l'assistant de duplication de groupe.

Supprimer un groupe

Vous pouvez supprimer un groupe d'administration lorsque vous souhaitez supprimer le groupe du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe admin supprime tous les utilisateurs du groupe, mais ne les supprime pas.

Étapes

1. Dans la page groupes, cochez la case correspondant à chaque groupe à supprimer.
2. Sélectionnez **actions > Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs dans StorageGRID

Lors de la création de groupes d'utilisateurs admin, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctions spécifiques de Grid Manager. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administration pour déterminer les tâches que l'utilisateur peut effectuer.

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au Grid Manager ou à l'API Grid Management.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds
- Afficher les alertes actuelles et résolues
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher certaines informations fournies sur les pages Configuration et Maintenance

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre **mode d'accès** du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administration. Toute fonctionnalité qui n'est pas explicitement mentionnée requiert l'autorisation **accès racine**.

Accès racine

Cette autorisation donne accès à toutes les fonctions d'administration de la grille.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **changer mot de passe root** de la page locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine local du locataire. Cette autorisation est également utilisée pour migrer les clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe root**.



Pour accorder l'accès à la page locataires, qui contient l'option **changer mot de passe racine**, attribuez également l'autorisation **comptes locataire**.

ILM

Cette autorisation permet d'accéder aux options de menu **ILM** suivantes :

- Règles
- Stratégies
- Balises de stratégie
- Pools de stockage
- Niveaux de stockage
- Régions

- Recherche de métadonnées d'objet



Les utilisateurs doivent disposer de l'autorisation **Autre configuration de grille** pour gérer les niveaux de stockage.

Maintenance

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser les options suivantes :

- **Configuration > Contrôle d'accès**
 - Mots de passe de grille
- **Configuration > Réseau**
 - Noms de domaine de terminaux S3
- **Maintenance > Tâches**
 - Désaffectation
 - De développement
 - Vérification de l'existence d'objet
 - Reprise après incident
- **Maintenance > Système**
 - Package de restauration
 - Mise à jour logicielle
- **Assistance > Outils**
 - Journaux

Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, les pages suivantes :

- **Maintenance > Réseau**
 - Serveurs DNS
 - Réseau Grid
 - Serveurs NTP
- **Maintenance > Système**
 - Licence
- **Configuration > Réseau**
 - Noms de domaine de terminaux S3
- **Configuration > Sécurité**
 - Certificats
- **Configuration > Surveillance**
 - Serveur d'audit et syslog

Gérer les alertes

Cette autorisation donne accès aux options de gestion des alertes. Les utilisateurs doivent disposer de cette

autorisation pour gérer les silences, les notifications d'alerte et les règles d'alerte.

Interrogation de metrics

Cette autorisation permet d'accéder aux éléments suivants :

- **Assistance > Outils > Page Métriques**
- Requêtes de metrics Prometheus personnalisées à l'aide de la section **Metrics** de l'API de gestion de grille
- Cartes de tableau de bord de Grid Manager qui contiennent des metrics

Recherche de métadonnées d'objet

Cette autorisation permet d'accéder à la page **ILM > recherche de métadonnées objet**.

Autre configuration de grille

Cette autorisation donne accès à ces options de configuration de grille supplémentaires :

- **ILM**
 - Niveaux de stockage
- **Configuration > Système**
- **Assistance > Autre**
 - Priorisation des E/S
 - Services de nœud
 - Seuils de stockage



Le coût du lien nécessite un accès root.

Administrateur de l'appliance de stockage

Cette autorisation permet :

- Accès à E-Series SANtricity System Manager sur les appliances de stockage via le gestionnaire de grid.
- Possibilité d'effectuer des tâches de dépannage et de maintenance dans l'onglet gérer les lecteurs pour les appliances prenant en charge ces opérations.

Comptes de locataires

Cette autorisation permet de :

- Accédez à la page tenants, où vous pouvez créer, modifier et supprimer des comptes de tenant
- Afficher les stratégies de classification du trafic existantes
- Affichez les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs dans StorageGRID

Vous pouvez afficher les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Créez un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et attribuer chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer des utilisateurs et des groupes fédérés.

Le Gestionnaire de grille inclut un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur racine.



Si l'authentification unique (SSO) est activée, les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Utilisateurs administrateurs**.
2. Sélectionnez **Créer utilisateur**.

Saisissez les informations d'identification de l'utilisateur

Étapes

1. Saisissez le nom complet de l'utilisateur, un nom d'utilisateur unique et un mot de passe.
2. Vous pouvez également sélectionner **Oui** si cet utilisateur ne doit pas avoir accès à Grid Manager ou à l'API de gestion de grille.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez éventuellement attribuer l'utilisateur à un ou plusieurs groupes pour déterminer les autorisations de l'utilisateur.

Si vous n'avez pas encore créé de groupes, vous pouvez enregistrer l'utilisateur sans sélectionner de groupes. Vous pouvez ajouter cet utilisateur à un groupe sur la page groupes.

Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir ["Gérez les groupes d'administration"](#) pour plus de détails.

2. Sélectionnez **Créer utilisateur** et **Terminer**.

Afficher et modifier les utilisateurs locaux

Vous pouvez afficher les détails des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour modifier son nom complet, son mot de passe ou son appartenance à un groupe. Vous pouvez

également empêcher temporairement un utilisateur d'accéder au Grid Manager et à l'API Grid Management.

Vous ne pouvez modifier que les utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau de la page utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou modifier le mot de passe d'un utilisateur local, utilisez le menu **actions** ou la page de détails.

Toutes les modifications sont appliquées la prochaine fois que l'utilisateur se déconnecte, puis se reconnecte au Grid Manager.



Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** de la bannière Grid Manager.

Tâche	Menu actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case de l'utilisateur. b. Sélectionnez actions > Afficher les détails de l'utilisateur .	Sélectionnez le nom de l'utilisateur dans le tableau.
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions > Modifier le nom complet . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône de modification  . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications .
Refuser ou autoriser l'accès StorageGRID	a. Cochez la case de l'utilisateur. b. Sélectionnez actions > Afficher les détails de l'utilisateur . c. Sélectionnez l'onglet accès. d. Sélectionnez Oui pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez non pour permettre à l'utilisateur de se connecter. e. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet accès. c. Sélectionnez Oui pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez non pour permettre à l'utilisateur de se connecter. d. Sélectionnez Enregistrer les modifications .

Tâche	Menu actions	Page de détails
Modifier le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions > Afficher les détails de l'utilisateur . c. Sélectionnez l'onglet Mot de passe. d. Saisissez un nouveau mot de passe. e. Sélectionnez changer mot de passe .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Saisissez un nouveau mot de passe. d. Sélectionnez changer mot de passe .
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions > Afficher les détails de l'utilisateur . c. Sélectionnez l'onglet groupes. d. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. e. Sélectionnez Modifier les groupes pour sélectionner différents groupes. f. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet groupes. c. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. d. Sélectionnez Modifier les groupes pour sélectionner différents groupes. e. Sélectionnez Enregistrer les modifications .

Importer des utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Utilisateurs administrateurs**.
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou plusieurs utilisateurs fédérés.

Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

- a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
- b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Importer les utilisateurs fédérés**.

Après avoir fermé la boîte de dialogue **Importer les utilisateurs fédérés**, les informations sur les utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur avec les mêmes autorisations.

Étapes

1. Cochez la case de l'utilisateur.
2. Sélectionnez **actions** > **Dupliquer utilisateur**.
3. Suivez l'assistant Dupliquer.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour supprimer définitivement cet utilisateur du système.



Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

1. Dans la page utilisateurs, cochez la case correspondant à chaque utilisateur à supprimer.
2. Sélectionnez **actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utilisation de la connexion unique (SSO)

Découvrez l'authentification unique StorageGRID

Lorsque l'authentification unique (SSO) est activée, les utilisateurs peuvent accéder à Grid Manager, Tenant Manager, Grid Management API ou Tenant Management API uniquement 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.

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) ou OpenID Connect.

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque l'authentification SSO est activée.

Connectez-vous lorsque SSO est activé

Lorsque l'authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

1. Entrez le nom de domaine complet ou l'adresse IP d'un nœud d'administration StorageGRID dans un navigateur Web.

La page de connexion StorageGRID s'affiche.

- Si c'est la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à saisir un identifiant de compte.
- Si vous avez déjà accédé au gestionnaire de grille ou au gestionnaire de locataires, vous êtes invité à sélectionner un compte récent ou à saisir un identifiant de compte.



La page de connexion StorageGRID n'apparaît pas lorsque vous entrez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivie 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 à l'aide de vos identifiants SSO](#).

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :

- Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
- Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.

3. Sélectionnez **connexion**

StorageGRID vous redirige vers la page de connexion SSO de votre entreprise. Par exemple :

4. Connectez-vous à l'aide de vos identifiants SSO.

Si vos informations d'identification SSO sont correctes :

- a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.
- b. StorageGRID valide la réponse d'authentification.
- c. Si la réponse est valide et que vous appartenez à un groupe fédéré avec des autorisations d'accès StorageGRID, vous êtes connecté au Gestionnaire de grille ou au Gestionnaire des locataires, selon le compte que vous avez sélectionné.



Si le compte de service est inaccessible, vous pouvez toujours vous connecter tant que vous êtes un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID.

5. Accédez éventuellement à d'autres nœuds d'administration ou à Grid Manager ou au tenant Manager, si vous disposez des autorisations adéquates.

Il n'est pas nécessaire de saisir à nouveau vos informations d'identification SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit où vous vous déconnectez.

Étapes

1. Localisez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

La page de connexion StorageGRID s'affiche. La liste déroulante **comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder plus rapidement à ces interfaces utilisateur à l'avenir.



Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration Remarque : si vous utilisez Entra ID pour l'authentification unique (SSO), 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
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.

Exigences et considérations relatives à l'authentification unique StorageGRID

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises et les considérations à prendre en compte.

Exigences du fournisseur d'identités

StorageGRID prend en charge plusieurs fournisseurs d'identité SSO (IdP).

OIDC

Les SSO suivants IdPs sont pris en charge pour OpenID Connect (OIDC) :

- Service de fédération Active Directory (AD FS)
- Identifiant Microsoft Entra
- Keycloak
- PingFederate
- Okta

SAML

Les SSO suivants IdPs sont pris en charge pour le langage de balisage d'assertion de sécurité 2.0 (SAML 2.0) :

- Service de fédération Active Directory (AD FS)
- Identifiant Microsoft Entra
- PingFederate

Vous devez configurer la fédération des identités de votre système StorageGRID avant de pouvoir configurer un fournisseur d'identités SSO. Le type de service LDAP que vous utilisez pour la fédération des identités contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Keycloak • Okta • ID d'entrée • PingFederate
ID d'entrée	ID d'entrée

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Système de fichiers AD Windows Server 2022
- Système de fichiers AD Windows Server 2019
- Système de fichiers AD Windows Server 2016



Windows Server 2016 doit utiliser le "[Mise à jour KB3201845](#)" ou une version ultérieure.

Supplémentaires requise

- TLS (transport Layer Security) 1.2 ou 1.3

- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Entra ID

Si vous utilisez Entra ID 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.

Configuration requise pour le certificat de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au 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 (Entra ID) 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 ["configuré un certificat personnalisé pour l'interface de gestion"](#) fait, vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID, les applications d'entreprise ou les connexions SP.



Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, d'une application d'entreprise ou d'un SP. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrices, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant dans le `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Configuration requise pour les ports

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique. Voir ["Contrôler l'accès au niveau du pare-feu externe"](#).

Confirmez que les utilisateurs fédérés peuvent se connecter à StorageGRID

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez déjà configuré la fédération des identités.

Étapes

1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.



Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

- a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
 - b. Sélectionnez **Gestion des accès > Fédération d'identité**.
 - c. Vérifiez que la case **Activer la fédération d'identité** n'est pas cochée.
 - d. Si c'est le cas, vérifiez que tous les groupes fédérés pouvant être utilisés pour ce compte de tenant ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
 - a. Depuis Grid Manager, sélectionnez **Configuration > Contrôle d'accès > Groupes d'administrateurs**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation d'accès racine.
 - c. Se déconnecter.
 - d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
 3. S'il existe des comptes de tenant existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès racine peut se connecter :
 - a. Dans 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 **utiliser le propre référentiel d'identité** est cochée, décochez la case et sélectionnez **Enregistrer**.

La page tenant s'affiche.

 - e. Sélectionnez le compte de tenant, sélectionnez **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.
 - f. Depuis le gestionnaire de locataires, sélectionnez **Gestion des accès > Groupes**.
 - g. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation d'accès racine pour ce locataire.
 - h. Se déconnecter.
 - i. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

- ["Configuration requise et considérations pour l'authentification unique"](#)
- ["Gérez les groupes d'administration"](#)
- ["Utilisez un compte de locataire"](#)

Découvrez comment configurer l'authentification unique (SSO) dans StorageGRID à l'aide d'OIDC

La mise en place de l'authentification unique (SSO) dans StorageGRID permet à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs.

Vous pouvez configurer l'authentification unique (SSO) dans StorageGRID à l'aide d'OpenID Connect (OIDC) ou de SAML. Suivez ces étapes générales pour configurer l'authentification unique (SSO) dans StorageGRID à l'aide d'OIDC ou découvrez "[Configuration de l'authentification unique \(SSO\) à l'aide de SAML](#)".

1

Configurer le fournisseur d'identité

En fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser, vous pouvez sélectionner Active Directory ou Entra ID pour le type de service LDAP de fédération d'identités.

- Pour Active Directory Federation Service (AD FS), vous pouvez utiliser le fournisseur d'identité AD FS, Entra ID, Keycloak, Okta ou PingFederate.
- Pour Entra ID, vous ne pouvez utiliser que le fournisseur d'identité Entra ID.

Utilisez le logiciel du fournisseur d'identité SSO pour configurer OIDC pour chaque nœud d'administration de votre grille.

- Découvrez "[création d'un groupe d'applications pour chaque nœud d'administration](#)" dans Active Directory
- Découvrez "[création d'une application pour chaque nœud d'administration](#)" dans Entra ID
- Découvrez "[création d'un client pour chaque nœud d'administration](#)" dans Keycloak
- Apprenez-en plus sur "[création d'une application Okta pour chaque nœud d'administration](#)"
- Apprenez-en plus sur "[création d'une connexion à un fournisseur de services pour chaque Admin Node](#)" PingFederate

2

Configurer l'authentification unique (SSO)

Sélectionnez l'assistant de configuration SSO pour OIDC. Configurez ensuite l'authentification unique (SSO) avec votre fournisseur d'identité et passez en mode sandbox pour configurer et tester l'authentification unique avant de l'activer pour les utilisateurs de StorageGRID.

Apprenez-en plus sur "[Configuration de l'authentification unique \(SSO\) à l'aide d'OIDC](#)"

3

Activer l'authentification unique (SSO)

Après avoir confirmé que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à chaque nœud d'administration, activez l'authentification unique pour tous les utilisateurs de StorageGRID.

Apprenez-en plus sur "[Activation de l'authentification unique \(SSO\) pour les utilisateurs de StorageGRID](#)"

Créez des groupes d'applications dans AD FS pour OIDC dans StorageGRID

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer un groupe d'applications pour chaque nœud d'administration pour OpenID Connect (OIDC) dans votre système.

Avant de commencer

- Vous disposez du domaine complet (ou de l'adresse IP) et de l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système.



Chaque nœud d'administration de votre système StorageGRID doit être associé à un groupe d'applications. Cela garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez créer un seul groupe d'applications pour tous les nœuds d'administration (recommandé) ou un groupe d'applications différent pour chaque nœud d'administration.

- Vous avez de l'expérience dans la création de groupes d'applications dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions concernent Windows Server 2022 AD FS. Si vous utilisez une autre version d'AD FS, vous constaterez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Étape 1 : Créer un groupe d'applications

Vous pouvez utiliser Windows PowerShell pour créer rapidement un groupe d'applications.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > AD FS Management**.
2. Sélectionnez **Groupes d'applications > Ajouter un groupe d'applications**
3. Pour **Nom**, saisissez l'identifiant de la partie de confiance.
4. Sous **Modèle**, sélectionnez **Applications client-serveur > Application serveur accédant à une API Web**.
5. Sélectionnez **Suivant**.
6. Enregistrez la valeur de l'**Client Identifier**.
7. Sous **URI de redirection**, saisissez le nom de domaine complet (ou l'adresse IP) `callback` et `logged-out` les URI pour le nœud d'administration :

◦ `https://<FQDN>/api/v4/oidc-callback` ou `https://<IP_address>/api/v4/oidc-callback`

◦ `https://<FQDN>/api/v4/oidc-logged-out` ou `https://<IP_address>/api/v4/oidc-logged-out`

Saisissez les URI de chaque nœud d'administration si vous utilisez un seul groupe d'applications pour tous les nœuds d'administration. Si vous utilisez un groupe d'applications différent pour chaque nœud d'administration, saisissez uniquement les URI du nœud d'administration correspondant.

8. Sélectionnez **Ajouter**.
9. Sélectionnez **Générer un secret partagé**, notez la valeur de **Secret**, puis sélectionnez **Suivant**.
10. Saisissez l'identifiant du client pour **Identifiant**.
11. Sélectionnez **Ajouter**, puis sélectionnez **Suivant**.
12. Sélectionnez **Autoriser tout le monde**.
13. Vérifiez que l'application serveur est sélectionnée sous **Application cliente (appelante)**.
14. Sous **Étendues autorisées**, vérifiez que seules les options suivantes sont sélectionnées :
 - allatclaims
 - e-mail
 - openid
 - profil
15. Sélectionnez **Suivant** > **Suivant**.
16. Sélectionnez **Fermer**.

Étape 2 : Configurer les règles de transformation d'émission

Configurez les règles de transformation d'émission pour chaque groupe d'applications.

Étapes

1. Dans la page **Gestion AD FS**, cliquez avec le bouton droit sur le groupe d'applications, puis sélectionnez **Propriétés**.
2. Sélectionnez l'API web créée précédemment, puis sélectionnez **Modifier**.
3. Sélectionnez **Règles de transformation d'émission** > **Ajouter une règle...**
4. Sous **Modèle de règle de revendication** :, sélectionnez **Envoyer l'attribut LDAP en tant que revendications**.
5. Sélectionnez **Suivant**.
6. Saisissez le nom d'une règle de revendication.
7. Sélectionnez **Active Directory** pour le magasin d'attributs.
8. Ajoutez les mappages d'attributs LDAP aux types de revendications sortantes :
 - E-Mail Addresses - E-Mail Address
 - Token-Groups - Unqualified Names - Group
9. Sélectionnez **Terminer**.
10. Sélectionnez **Appliquer** > **OK** > **OK**.

Et ensuite

Après avoir créé des groupes d'applications, "[Configurer l'authentification unique \(SSO\) à l'aide d'OIDC](#)".

Créez des applications d'entreprise dans Entra ID pour OIDC dans StorageGRID

Utilisez Entra ID pour créer une application d'entreprise pour chaque nœud d'administration pour OpenID Connect (OIDC) dans votre système.

Avant de commencer

- Vous disposez de l'identifiant de la partie de confiance et du domaine complet (FQDN) ou de l'adresse IP pour chaque nœud d'administration de votre système.



Chaque nœud d'administration de votre StorageGRID doit disposer d'une application d'entreprise. Cela garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez créer une seule application d'entreprise pour tous les nœuds d'administration (recommandé) ou une application d'entreprise différente pour chaque nœud d'administration.

- Vous avez de l'expérience dans la création d'applications dans Entra ID.
- Vous disposez d'un compte Entra ID avec un abonnement actif.
- Vous disposez de l'un des rôles suivants dans le compte Entra ID : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal de service.

Étape 1 : Accédez à Entra ID

Étapes

1. Connectez-vous au "[Portail Azure](#)".
2. Sélectionnez "[Identifiant Microsoft Entra](#)".
3. Sélectionnez "[Enregistrements d'application](#)".

Étape 2 : Enregistrer une nouvelle application

Enregistrez une nouvelle application d'entreprise pour chaque nœud d'administration de votre système.

Étapes

1. Dans le volet Applications d'entreprise d'Entra ID, sélectionnez **Inscriptions d'applications > Nouvelle inscription**.
2. Pour **Nom**, saisissez l'identifiant de la partie de confiance.
3. Sous **Types de comptes pris en charge**, sélectionnez les types de comptes qui peuvent utiliser l'application ou accéder à l'API, par exemple, **Locataire unique uniquement - <tenant_name>**.
4. Sous **URI de redirection**, sélectionnez **Sélectionner une plateforme > Web**.
5. Saisissez l'URI de redirection FQDN (ou adresse IP) pour le nœud d'administration : <https://<FQDN>/api/v4/oidc-callback> ou https://<IP_address>/api/v4/oidc-callback

Saisissez l'URI de chaque nœud d'administration si vous utilisez une seule application d'entreprise pour tous les nœuds d'administration. Si vous utilisez une application d'entreprise différente pour chaque nœud d'administration, saisissez uniquement l'URI du nœud d'administration correspondant.
6. Sélectionnez **Register**.
7. Sur la page Vue d'ensemble de l'enregistrement de la nouvelle application, notez l'**ID de l'application (client)** et l'**ID du répertoire (tenant)**.

Étape 3 : Configurer un secret client

Enregistrez un secret client pour chaque nouvelle application.

Étapes

1. Sur la page Vue d'ensemble de l'enregistrement de la nouvelle application, sélectionnez **Gérer >**

Certificats et secrets > Nouveau secret client.

2. Saisissez le code secret du client et définissez une date d'expiration souhaitée.
3. Sélectionnez **Ajouter** pour créer le secret client.
4. Copiez la **valeur** secrète.



La valeur secrète n'est plus visible après une actualisation ou après avoir quitté la page du secret client.

Étape 4 : Configurer les autorisations de l'API

Configurez les autorisations API pour chaque nouvelle application.

Étapes

1. Sur la page Vue d'ensemble de l'enregistrement de la nouvelle application, sélectionnez **Gérer > Autorisations API > Ajouter une autorisation**.
2. Sélectionnez **Microsoft APIs > Microsoft Graph > Autorisations déléguées**.
3. Développez **OpenId permissions**, puis sélectionnez **email, offline_access, openid** et **profile**.
4. Sélectionnez **Ajouter des autorisations**.
5. Sélectionnez **Accorder le consentement de l'administrateur pour <tenant>**, puis sélectionnez **Oui**.

Étape 5 : Ajouter l'URI de redirection de l'utilisateur déconnecté

Ajoutez l'URI de redirection après déconnexion pour chaque nouvelle application.

Étapes

1. Sur la page Vue d'ensemble de l'enregistrement de la nouvelle application, sélectionnez **Gérer > Authentification**.
2. Sélectionnez **Ajouter un URI de redirection > Web**.
3. Saisissez l'URI de redirection FQDN (ou adresse IP) pour le nœud d'administration : `https://<FQDN>/api/v4/oidc-logged-out` ou `https://<IP_address>/api/v4/oidc-logged-out`

Saisissez l'URI de chaque nœud d'administration si vous utilisez un seul groupe d'applications pour tous les nœuds d'administration. Si vous utilisez un groupe d'applications différent pour chaque nœud d'administration, saisissez uniquement l'URI du nœud d'administration correspondant.

4. Sélectionnez **Configurer**.

Et ensuite

Après la création d'applications d'entreprise, "[Configurer l'authentification unique \(SSO\) à l'aide d'OIDC](#)".

Créez des clients dans Keycloak pour OIDC dans StorageGRID

Utilisez Keycloak pour créer une connexion client pour chaque nœud d'administration pour OpenID Connect (OIDC) dans votre système StorageGRID.

Avant de commencer

- Vous avez de l'expérience dans la création de clients dans Keycloak, ou vous avez accès à la documentation Keycloak.

- Vous disposez d'un compte dédié (Bind DN) pour les recherches d'annuaire et les informations d'identification de connexion.
- Vous disposez d'un accès administrateur Keycloak.

Description de la tâche

Chaque nœud d'administration de votre système StorageGRID doit disposer d'une connexion client. Cela garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez créer une seule connexion client pour tous les nœuds d'administration (recommandé) ou une connexion client différente pour chaque nœud d'administration.

Utilisez les paramètres par défaut, sauf indication contraire. Dans certains cas, vous pouvez utiliser les paramètres requis par votre organisation.

Étape 1 : Facultativement, créez un realm

Créez un realm Keycloak pour configurer le fournisseur LDAP et le client OIDC, ou utilisez le realm par défaut de Keycloak.

Étapes

1. Sélectionnez **Créer un royaume**.
2. Saisissez un nom pour le royaume.
3. Sélectionnez **Activé**.
4. Sélectionnez **Créer**.

Étape 2 : Configurer le fournisseur LDAP

Configurez le fournisseur LDAP afin que Keycloak se connecte au serveur LDAP du service de fédération Active Directory Federation Service (AD FS).

Étapes

1. Sélectionnez **Fédération d'utilisateurs > Ajouter des fournisseurs LDAP**.
2. Sous l'onglet Paramètres :
 - a. Saisissez les valeurs recommandées suivantes :
 - Nom d'affichage dans l'interface utilisateur : Saisissez une valeur unique.
 - Fournisseur : **Active Directory**
 - URL de connexion : `ldap://<ldap_IP_address>` ou `ldaps://<ldap_IP_address>`
 - Mise en commun des connexions : **ON**
 - DN de liaison : Saisissez votre DN de liaison
 - Identifiants de connexion : saisissez le mot de passe
 - Mode édition : **READ_ONLY**
 - DN des utilisateurs : Par exemple, `CN=Users, DC=saml, DC=sgws`
 - Attribut LDAP du nom d'utilisateur : **sAMAccountName**
 - Attribut LDAP RDN : **cn**
 - Attribut LDAP UUID : **objectGUID**
 - Classes d'objets utilisateur : `person, organizationalPerson, user`

- Filtre LDAP utilisateur : (sAMAccountName=*)
- Étendue de la recherche : **Sous-arbre**
- Pagination : **ACTIVÉE**
- Importer des utilisateurs : **ACTIVÉ**
- Enregistrements de synchronisation : **ACTIVÉ**
- Supprimez les utilisateurs invalides lors des recherches : **ACTIVÉ**

b. Sélectionnez **Tester la connexion** et **Tester l'authentification**.

Réglez tout problème éventuel avant de continuer.

3. Sélectionnez **Enregistrer**.

Étape 3 : Configurer le mappage LDAP

Configurez le mappage LDAP pour associer AD en tant qu'attribut à Keycloak.

Étapes

1. Accédez à **Fédération d'utilisateurs > LDAP**
2. Sélectionnez **fournisseur LDAP** que vous avez créé.
3. Dans l'onglet Mappers, sélectionnez **Add mapper > Create new mapper**.
4. Pour le type de Mapper, sélectionnez **user-attribute-ldap-mapper**.
5. Sélectionnez **Enregistrer**, puis saisissez les informations suivantes :
 - Attribut du modèle utilisateur : **userPrincipalName**
 - Attribut LDAP : **userPrincipalName**
 - Lecture seule : **ON**
 - Toujours lire la valeur depuis LDAP : **ACTIVÉ**
 - Obligatoire dans LDAP : **OFF**
 - Forcer une valeur par défaut : **ON**
 - Attribut binaire : **DÉSACTIVÉ**
6. Sélectionnez **Enregistrer**.

Étape 4 : Créez un client OIDC

Créez le client OIDC pour votre système.

Étapes

1. Accédez à **Clients > Create client**.
2. Pour les paramètres généraux, saisissez les informations suivantes :
 - Nom : Saisissez un nom d'affichage pour le client.
 - Type de client : **OIDC Connect**
 - ID client : Saisissez une valeur unique. Conservez cette valeur pour une utilisation ultérieure.
3. Sélectionnez **Suivant**.

4. Pour la configuration des capacités, saisissez les informations suivantes :

- Authentification du client : **ON**
- Flux standard : **Activer**
- Autorisations d'accès direct : **Activer**
- Rôles du compte de service : **Enable**

5. Sélectionnez **Suivant**.

6. Pour les paramètres de connexion, saisissez les URI de redirection :



Si un ou plusieurs points de terminaison d'équilibrage de charge sont configurés pour l'interface de gestion, ajoutez les URI de redirection pour chaque port. Par exemple :
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` et
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

- URI de redirection valides : `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback` et `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- URI de redirection valides après déconnexion :
`https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- Origines du Web `https://<Admin_IP_address_or_FQDN>`

7. Sélectionnez **Enregistrer**.

Étape 5 : Générer le secret client

Générez un secret client pour le client OIDC que vous avez créé.

Étapes

1. Allez dans **Clients**, puis sélectionnez le **Client OIDC** que vous avez créé.
2. Dans l'onglet Identifiants, saisissez les informations suivantes :
 - Authentificateur client : **Client Id et Secret**
 - Secret client : **Générez ou définissez un secret client**. Enregistrez cette valeur pour une utilisation ultérieure.

Étape 6 : Définir les portées

Définissez les portées dans Keycloak.

Étapes

1. Accédez à **Étendues client** > **Créer une étendue client**, puis saisissez les informations suivantes :
 - Type : **Aucun**
 - Protocole : **OpenID Connect**
 - Afficher sur l'écran de consentement : **Activé**
 - Inclure dans les métadonnées du fournisseur OpenID : **Activé**
2. Sélectionnez **Enregistrer**.
3. Dans l'onglet Mappers, sélectionnez **Configurer un nouveau mappeur** > **Attribut utilisateur**, puis saisissez les informations suivantes :

- Nom : Saisissez une valeur unique.
- Attribut utilisateur : **userPrincipalName**
- Nom de la revendication du jeton : **upn**
- Type JSON de la revendication : **String**
- Ajouter au jeton d'identification : **ON**
- Ajouter au jeton d'accès : **ON**
- Ajouter aux informations utilisateur : **ACTIVÉ**
- Ajouter à l'introspection des jetons : **ON**

4. Sélectionnez **Enregistrer**.

5. Allez dans **Clients** et sélectionnez le **Client OIDC** que vous avez créé.

6. Sélectionnez **Étendues client > Ajouter une étendue client**.

7. Sélectionnez le périmètre client que vous avez créé.

8. Sélectionnez **Ajouter**.

Étape 7 : Préparez-vous à configurer l'authentification unique (SSO) à l'aide d'OIDC

Enregistrez les informations nécessaires à la configuration de l'authentification unique (SSO) avec OIDC à l'aide de Keycloak dans votre système StorageGRID.

Étapes

1. Vérifiez que vous avez enregistré le **ID client** et le **secret client** du client OIDC que vous avez créé.
2. Enregistrez le point de terminaison de découverte OpenID Connect pour le domaine. Celui-ci est disponible dans le point de terminaison de configuration `well-known` :

```
https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/well-known/openid-configuration
```

Incluez éventuellement le port réseau :

```
https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>/well-known/openid-configuration
```

Et ensuite

Après avoir créé des clients OIDC, "[Configurer l'authentification unique \(SSO\) à l'aide d'OIDC](#)".

Créer une application Okta pour OIDC dans StorageGRID

Créez une application Okta pour tous les nœuds d'administration pour OpenID Connect (OIDC) dans votre système StorageGRID.

Avant de commencer

- Vous avez de l'expérience dans la création d'applications Okta, ou vous avez accès à la documentation Okta.
- Vous disposez d'un accès administrateur Okta.

Description de la tâche

Une application Okta doit contenir des URI de redirection de connexion et de déconnexion pour tous les nœuds d'administration. Les URI de redirection garantissent que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez créer une seule application Okta pour tous les nœuds d'administration (recommandé) ou une application différente pour chaque nœud d'administration.

Utilisez les paramètres par défaut, sauf indication contraire. Dans certains cas, vous pouvez utiliser les paramètres requis par votre organisation.

Étape 1 : Créer une application Okta

Créez une application Okta à l'aide de l'interface utilisateur Okta.

Étapes

1. Dans Okta, allez dans **Applications > Applications**.
 2. Sélectionnez **Créer une intégration d'application**, puis saisissez les informations suivantes :
 - Méthode de connexion : **OIDC - OpenID Connect**
 - Type d'application : **Application Web**
 3. Sélectionnez **Suivant**.
 4. Saisissez un nom pour l'application dans le champ Intégration d'application.
 5. Vérifiez que l'option Authorization Code est sélectionnée (par défaut) pour les Core grants.
 6. Ajoutez les URI de redirection de connexion et de déconnexion pour chaque nœud d'administration :
 - URI de redirection de connexion : `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
 - URI de redirection de déconnexion : `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- 
- Si un ou plusieurs points de terminaison d'équilibrage de charge sont configurés pour l'interface de gestion, ajoutez les URI de redirection pour chaque port. Par exemple :
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` et
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

Étape 2 : Ajouter un groupe fédéré

Créez un groupe ou utilisez un groupe existant à partir du serveur Active Directory Federation Service (AD FS) pour StorageGRID.

Étapes

1. Dans GRID Manager, sélectionnez **Configuration > Groupes d'administration > Créer un groupe > Groupe fédéré**.
2. Saisissez le nom du groupe de serveurs AD FS.
3. Sélectionnez **Lecture-écriture** pour le mode d'accès et **Accès racine** pour les autorisations.
4. Sélectionnez **Créer groupe**.

Étape 3 : Importer les groupes et les utilisateurs du serveur AD FS

Installez le client Okta Active Directory sur le serveur AD FS. Ensuite, importez les groupes et les utilisateurs du serveur AD FS.

Étapes

1. Dans Okta, allez dans **Répertoire > Intégrations de répertoire > Ajouter un répertoire > Ajouter Active Directory**.
2. Sélectionnez **Configurer Active Directory > Télécharger l'agent**.
3. Suivez immédiatement la procédure d'installation.



Si vous tardez, l'installation risque de s'interrompre et vous devrez recommencer.

- a. Sélectionnez le domaine Active Directory.
 - b. Créez un compte OktaService au lieu de lier un utilisateur existant.
 - c. Sélectionnez les unités organisationnelles qui contiennent les utilisateurs et les unités organisationnelles qui contiennent les groupes.
 - d. Sélectionnez le nom d'utilisateur principal (UPN) qui utilise l'UPN Active Directory comme nom d'utilisateur Okta. Par exemple : `user@domain.com`
4. Recherchez l'application **Okta AD Agent Management Utility**. Ensuite, exécutez l'application et confirmez que le message d'état `The agent is running` apparaît.



Le client Okta AD doit être en cours d'exécution chaque fois que vous souhaitez effectuer une synchronisation et une importation de serveur AD FS avec Okta.

5. Dans Okta, allez dans **Répertoire > Intégrations de répertoire**.
6. Sélectionnez l'intégration de répertoire que vous avez créée.
7. Sélectionnez **Importer > Importer maintenant**.
8. Sélectionnez l'utilisateur que vous souhaitez importer, puis sélectionnez **Confirmer les affectations**.
9. Allez dans **Répertoire > Personnes** et confirmez que l'utilisateur a été importé avec succès.

Si le statut de l'utilisateur n'est pas Actif, sélectionnez **Activer** et continuez d'actualiser la page jusqu'à ce que l'utilisateur ait le statut Actif.

10. Accédez à **Répertoire > Groupes** et confirmez que le groupe de l'utilisateur importé a été importé automatiquement.
11. Sélectionnez le groupe et vérifiez que l'utilisateur importé fait partie de ce groupe.

Étape 4 : Configurer une revendication

Configurez une revendication pour inclure les groupes de serveurs AD FS dans le jeton d'accès. Vérifiez ensuite que la revendication inclut le groupe importé pour l'utilisateur importé et l'application Okta.

Étapes

1. Dans Okta, allez dans **Directory > Groups**.
2. Sélectionnez le groupe importé pour l'utilisateur importé.
3. Sélectionnez **Applications > Attribuer des applications > Attribuer**.

4. Accédez à **Sécurité > API**.
5. Sélectionnez le serveur d'autorisation **par défaut**.
6. Sélectionnez **Claims > Add Claim**. Ensuite, créez une réclamation avec les informations d'identification suivantes :
 - Nom : **groups**
 - Inclure dans le type de jeton : **ID Token - Toujours**
 - Type de valeur : **Expression**
 - Valeur : **Groups.startsWith("active_directory","",100)**
 - Inclure dans : **Toute portée**
7. Accédez à **Sécurité > API**.
8. Sélectionnez le serveur d'autorisation **par défaut**.
9. Sélectionnez l'onglet **Aperçu du jeton** et saisissez les informations d'identification suivantes pour les propriétés de la requête :
 - Client OAuth/OIDC : **<application name>**
 - Type d'autorisation : **Code d'autorisation**
 - Utilisateur : **Utilisateur importé (adresse e-mail)**
 - Scopes : **courriel, profil, openid**
10. Sélectionnez **Exécuter**.

Le groupe importé apparaît dans l'onglet Preview id_token de la charge utile.

Et ensuite

Après avoir créé une application Okta, "[Configurer l'authentification unique \(SSO\) à l'aide d'OIDC](#)".

Créez des connexions de fournisseur de services dans PingFederate pour OIDC dans StorageGRID

Utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration pour OpenID Connect (OIDC) dans votre système.

Avant de commencer

- Vous avez l'expérience de la création de connexions SP dans PingFederate Server.
- Vous avez le "[Guide de référence de l'administrateur](#)" serveur for PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous avez le "[Autorisation d'administrateur](#)" pour le serveur PingFederate.

Description de la tâche

Ces instructions résument comment configurer le serveur PingFederate version 12.1.10 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Consultez la documentation du serveur PingFederate pour obtenir des instructions détaillées concernant votre version.

Utilisez les paramètres par défaut, sauf indication contraire. Dans certains cas, vous pouvez utiliser les paramètres requis par votre organisation, tels que les paramètres de méthode d'authentification.

Étape 1 : Créez 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.

Étapes

1. Accédez à **Système > Magasins de données et d'identifiants**.
2. Sélectionnez **New Data Store**.
3. Pour le type, sélectionnez **Directory (LDAP)**.
4. Sélectionnez **Suivant**.
5. Sous Configuration LDAP :
 - Saisissez les valeurs pour **Hostname**, **User DN** (username) et **Password**.

Utilisez les valeurs que vous avez utilisées lors de "[configuration de la fédération des identités](#)" dans StorageGRID.

- Pour Active Directory, sélectionnez **Type LDAP**.

Étape 2 : Créer un validateur d'identifiant de mot de passe

Si ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

Étapes

1. Sélectionnez **Password Credential Validators > Create New instance**.
2. Dans l'onglet Type, saisissez les informations suivantes :
 - a. NOM DE L'INSTANCE et ID DE L'INSTANCE : Vous pouvez utiliser la même valeur pour les deux.
 - b. Type : sélectionnez **LDAP Username Password Credential Validator**.
3. Sélectionnez **Suivant**.
4. Dans l'onglet Configuration de l'instance, saisissez les informations suivantes :
 - LDAP DATASTORE : Sélectionnez le [magasin de données](#) que vous avez créé.
 - BASE DE RECHERCHE : Saisissez les informations pour le [Configuration LDAP](#).
 - FILTRE DE RECHERCHE : Saisissez **sAMAccountName=\${username}**.
 - ÉTENDUE DE LA RECHERCHE : sélectionnez **Sous-arbre**.
5. Sélectionnez **Suivant**.
6. Dans l'onglet Contrat étendu, ajoutez les attributs suivants : `memberOf`, `objectGUID`, `sAMAccountName`, `sn`, et `userPrincipalName`.
7. Sélectionnez **Suivant > Enregistrer**.

Étape 3 : Créez une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP (identity provider).



Chaque nœud d'administration de votre StorageGRID doit avoir une connexion IdP. Cela garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez créer une seule connexion IdP pour tous les nœuds d'administration (recommandé) ou une connexion IdP différente pour chaque nœud d'administration.

Étapes

1. Accédez à **Authentication > Integration > IDP Adapters**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, saisissez les informations suivantes :
 - NOM DE L'INSTANCE et ID DE L'INSTANCE : Vous pouvez utiliser la même valeur pour les deux.
 - TYPE : Sélectionnez **HTML Form IdP Adapter**.
4. Sélectionnez **Suivant**.
5. Dans l'onglet **Adaptateur IdP**, sélectionnez **Ajouter une nouvelle ligne à 'Credential Validators'**.
6. Sélectionnez [validateur des informations d'identification du mot de passe](#) que vous avez créé.
7. Sélectionnez **Suivant**.
8. Dans l'onglet Contrat étendu, ajoutez les attributs que vous avez mappés pour le [validateur des informations d'identification du mot de passe](#).
9. Sélectionnez **Suivant**.
10. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour Pseudonym.
11. Sélectionnez **Suivant > Suivant**.
12. Vérifiez le résumé et sélectionnez **Enregistrer**.

Étape 4 : Configurer les paramètres du serveur OAuth et du serveur d'autorisation

Configurez le serveur d'autorisation pour prendre en charge les types d'autorisation acceptés par StorageGRID.

Étapes

1. Accédez à **Système > Paramètres du serveur d'autorisation**.
2. Vérifiez que les options suivantes sont sélectionnées pour REUSE EXISTING PERSISTENT ACCESS GRANTS FOR GRANT TYPES :
 - IMPLICITE
 - CODE D'AUTORISATION
 - IDENTIFIANT DE MOT DE PASSE DU PROPRIÉTAIRE DE LA RESSOURCE



Si votre entreprise restreint l'utilisation des IDENTIFIANTS DE MOT DE PASSE DU PROPRIÉTAIRE DE LA RESSOURCE, vous ne pouvez utiliser que le CODE D'AUTORISATION.

3. Pour les paramètres des services Web administratifs OAuth, sélectionnez [validateur des informations d'identification du mot de passe](#) que vous avez créé.

Étape 5 : Définir les portées

Définissez les portées dans PingFederate.

Étapes

1. Accédez à **Système > Paramètres OAuth > Gestion de l'étendue**.
2. Dans l'onglet Common Scopes, ajoutez les valeurs pour **openid**, **email** et **profile**, si elles n'existent pas déjà.

Étape 6 : Configurer le mappage de l'adaptateur IdP

Configurez le mappage de l'adaptateur IdP pour associer les attributs de l'IdP aux autorisations persistantes délivrées aux clients, telles que les jetons d'accès ou les jetons d'actualisation.

Étapes

1. Accédez à **Authentification > Mappage des contrats de stratégie d'autorisation**.
2. Sélectionnez **Mappage des autorisations de l'adaptateur IdP**.
3. Dans la liste déroulante INSTANCE D'ADAPTATEUR SOURCE, sélectionnez [Adaptateur de formulaire HTML](#) celle que vous avez créée.
4. Sélectionnez **Ajouter un mappage > Contract Fulfillment**.
5. Sous Source, sélectionnez **Adapter** pour USER_KEY et USER_NAME.
6. Sous Valeur, sélectionnez **sAMAccountName** pour USER_KEY et **username** pour USER_NAME.
7. Sélectionnez **Suivant > Suivant** pour accéder à la page récapitulative.
8. Sélectionnez **Enregistrer**.

Étape 7 : Configurer le mappage des identifiants du propriétaire de la ressource

Configurez le mappage des identifiants du propriétaire de la ressource pour garantir que les identifiants de l'utilisateur sont correctement validés lors de l'authentification.

Étapes

1. Accédez à **Authentification > Mappage des contrats de stratégie d'autorisation**.
2. Sélectionnez **Mappage des identifiants du propriétaire de la ressource**.
3. Dans la liste déroulante SOURCE PASSWORD VALIDATOR INSTANCE, sélectionnez [validateur des informations d'identification du mot de passe](#) que vous avez créée.
4. Sélectionnez **Ajouter un mappage > Contract Fulfillment**.
5. Ajoutez le mappage pour USER_KEY :
 - Sous Source, sélectionnez **Password Credential Validator**.
 - Sous Valeur, sélectionnez **sAMAccountName**.
6. Sélectionnez **Suivant > Suivant** pour accéder à la page récapitulative.
7. Sélectionnez **Enregistrer**.

Étape 8 : Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **sécurité > clés de signature et de déchiffrement**.
2. Sélectionnez **Créer nouveau**, puis saisissez les informations suivantes :
 - Nom commun (CN) : Il doit s'agir du domaine complet (FQDN) du serveur.
 - Organisation (Org) : Saisissez le nom de votre organisation.
 - Pays : Indiquez le code pays à deux lettres, par exemple US pour les États-Unis.
 - Algorithme de clé : sélectionnez l'algorithme de clé approprié, tel que **RSA**.
 - Taille de la clé : définie sur **2048** bits.
 - Algorithme de signature : Sélectionnez **RSA avec SHA256** comme algorithme de signature pour garantir des opérations cryptographiques sécurisées.

Étape 9 : Configurer la gestion des jetons d'accès

StorageGRID utilise des jetons d'accès pour authentifier et autoriser les requêtes API dans PingFederate.

Étapes

1. Accédez à **Applications > Gestion des jetons d'accès**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, saisissez les informations suivantes :
 - NOM DE L'INSTANCE et ID DE L'INSTANCE : Vous pouvez utiliser la même valeur pour les deux.
 - Type : Vérifiez que la valeur est **JSON Web Tokens**.
4. Sélectionnez **Suivant**.
5. Dans l'onglet Configuration de l'instance, saisissez les informations suivantes pour les certificats :
 - ID DE CLÉ : Saisissez un identifiant unique pour la clé.
 - Certificat : Ajoutez le [certificat](#) que vous avez créé.
 - ALGORITHME JWS : sélectionnez **RSA using SHA256**.
 - ID DE CLÉ DU CERTIFICAT DE SIGNATURE ACTIF : Sélectionnez l'**ID DE CLÉ** que vous avez créé à cette étape.
6. Sélectionnez **Suivant > Suivant**.
7. Dans l'onglet Contrat d'attribut de jeton d'accès, sélectionnez **USER_KEY** pour Nom de l'attribut du sujet et **username** pour Étendre le contrat.
8. Sélectionnez **Ajouter**.
9. Sélectionnez **Suivant > Suivant > Suivant** pour accéder à la page récapitulative.
10. Sélectionnez **Enregistrer**.

Étape 10 : Configurer le mappage des jetons d'accès

Configurez le mappage des jetons d'accès pour utiliser le jeton d'accès que vous avez créé.

Étapes

1. Accédez à **Applications > Mappages de jetons d'accès**.
2. Sélectionnez **Mappages de jetons d'accès**.
3. Sélectionnez **Ajouter un mappage**.

4. Pour le contexte, sélectionnez **Default**.
5. Pour le Gestionnaire de jetons d'accès, sélectionnez le [jeton d'accès](#) que vous avez créé.
6. Sélectionnez **Suivant > Exécution du contrat** :
7. Sous Source, sélectionnez **Persistent Grant** pour le nom d'utilisateur.
8. Sous Valeur, sélectionnez **USER_KEY** pour le nom d'utilisateur.
9. Sélectionnez **Suivant > Enregistrer**.

Étape 11 : Configurer la politique OpenID Connect

Définissez les politiques OpenID Connect pour l'accès client aux attributs qui sont mappés conformément aux spécifications OpenID.

Étapes

1. Accédez à **Applications > Clients OAuth**.
2. Sélectionnez **Openid Connect Policy Management > Add Policy**.
3. Dans l'onglet Gérer la stratégie, saisissez les informations suivantes :
 - ID DE LA POLITIQUE : Un identifiant unique pour la politique.
 - NOM DE LA STRATÉGIE : Un nom descriptif pour la stratégie.
 - GESTIONNAIRE DE JETONS D'ACCÈS : Sélectionnez le [jeton d'accès](#) que vous avez créé.
 - DURÉE DE VIE DU JETON D'IDENTIFICATION : Définissez la durée de vie souhaitée pour le jeton d'identification, par exemple 60 minutes ou une heure.
 - INCLURE LES INFORMATIONS UTILISATEUR DANS LE JETON D'IDENTIFICATION : Cochez la case pour inclure les informations de l'utilisateur dans le jeton d'identification.
4. Sélectionnez **Suivant**.
5. Dans l'onglet Contrat d'attributs, supprimez tous les attributs existants qui ne sont pas nécessaires pour le [magasin de données](#) que vous avez créé. Ne conservez que les attributs que vous souhaitez transmettre de Ping Authentication à StorageGRID.



Il s'agit d'une étape cruciale. Elle détermine les valeurs d'attribut incluses dans le jeton d'identification. StorageGRID hérite de ces valeurs lors du processus d'authentification.

6. Sélectionnez **Suivant > Suivant**.
7. Dans l'onglet Source d'attributs et recherche d'utilisateurs, sélectionnez **Ajouter une source d'attributs**. Saisissez ensuite les informations suivantes :
 - ID DE LA SOURCE D'ATTRIBUT et DESCRIPTION DE LA SOURCE D'ATTRIBUT : Vous pouvez utiliser la même valeur pour les deux.
 - MAGASIN DE DONNÉES ACTIF : Sélectionnez le [magasin de données](#) que vous avez créé.
8. Sélectionnez **Suivant**.
9. Dans l'onglet LDAP Directory Search :
 - a. Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
 - b. Dans la liste déroulante ROOT OBJECT CLASS, sélectionnez **objectClass**.
 - c. Dans la liste déroulante ATTRIBUTE, ajoutez un attribut pour chaque classe d'objet que vous

souhaitez mapper. Par exemple :

- **InetOrgPerson** : Ajoutez `displayName`, `givenName` ou `HomePhone`.
- **utilisateur** : Ajoutez `LocalID` ou `userPrincipalName` (`upn`).
- **En haut** : Ajoutez `memberOf` ou `nom`.
- **person** : Ajouter `sn`.

10. Sélectionnez **Suivant**.

11. Dans l'onglet filtre LDAP, entrez **sAMAccountName=\${username}**.

Vous devez personnaliser le filtre LDAP pour que StorageGRID récupère les attributs utilisateur en fonction de la structure Active Directory ou LDAP spécifique à votre organisation. Consultez votre administrateur LDAP/AD pour obtenir l'expression de filtre appropriée à votre configuration.

12. Sélectionnez **Enregistrer** et consultez le résumé.

13. Dans l'onglet Exécution du contrat, saisissez les informations suivantes :

- **Source** : Sélectionnez le [base de données LDAP](#) que vous avez créé.
- **Valeur** : Associez chaque contrat d'attribut à la valeur correspondante.

14. Sélectionnez **Suivant** > **Suivant**.

15. Vérifiez le résumé et sélectionnez **Enregistrer**.

16. Accédez à **Applications** > **Clients OAuth** > **Gestion des politiques OpenID Connect**.

17. Vérifiez que la stratégie que vous avez créée est définie comme stratégie par défaut.

Étape 12 : Créer un client OAuth pour le serveur OAuth

Créez un nouveau client OAuth pour configurer les informations d'identification client nécessaires et autoriser les connexions entre PingFederate et StorageGRID.

Étapes

1. Accédez à **Applications** > **Clients OAuth**.

2. Sélectionnez **Add Client**, puis saisissez les informations suivantes :

- **ID CLIENT** : Saisissez une valeur unique.
- **AUTHENTIFICATION DU CLIENT** : sélectionnez **Client Secret**.
- **SECRET CLIENT** : Sélectionnez **MODIFIER LE SECRET** > **Générer le secret**.

Cela génère la clé secrète du client. Conservez cette clé pour une utilisation ultérieure.

- **URI DE REDIRECTION** : Indiquez les URL de retour StorageGRID dans la section **URI de redirection**. Ces URL doivent correspondre aux URL configurées dans StorageGRID pour OAuth : par exemple :
 - `https://<Admin IP or Hostname>/api/v4/oidc-callback`
 - `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
- **TYPES DE SUBVENTIONS AUTORISÉES** : Sélectionnez les options suivantes :
 - **Code d'autorisation** : Ceci lance le flux OAuth.
 - **Jeton d'actualisation** : Obtenez un nouveau jeton lorsqu'un jeton d'accès expire.
 - **Identifiants du propriétaire de la ressource** : Si vous avez besoin d'un accès direct aux identifiants de l'utilisateur pour l'authentification.

- OPENID CONNECT : Sélectionnez **RSA using SHA-256** pour l'algorithme de signature du jeton d'identification.
- Mode de déconnexion : sélectionnez **OIDC Back-Channel**.
- URI de déconnexion du canal frontal, URI de déconnexion du canal dorsal et URI de redirection post-déconnexion : ajoutez l'URI de déconnexion StorageGRID : `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

3. Sélectionnez **Enregistrer**.

Et ensuite

Après avoir créé les connexions SP, "[Configurer l'authentification unique \(SSO\) à l'aide d'OIDC](#)".

Configurer l'authentification unique (SSO) dans StorageGRID à l'aide d'OIDC

Suivez l'assistant de configuration SSO pour OpenID Connect (OIDC) et passez en mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID. Après avoir activé l'authentification unique, vous pouvez revenir en mode sandbox si nécessaire pour modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Autorisation d'accès racine](#)".
- Vous avez configuré le client OIDC dans le fournisseur d'identité SSO de votre système StorageGRID.
- Vous avez "[fédération des identités configurée](#)" pour votre système StorageGRID.

Étape 1 : Fournir les détails du fournisseur d'identité

Accédez à l'assistant et complétez les champs de la page Fournir les détails du fournisseur d'identité.

Étapes

1. Accédez à l'assistant pour configurer les paramètres SSO :

- Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**. La page d'authentification unique apparaît.



Si le bouton Configurer les paramètres SSO est désactivé, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. "[Configuration requise et considérations pour l'authentification unique](#)".

- Sélectionnez **Configurer les paramètres SSO**. La page Fournir les détails du fournisseur d'identité s'affiche.

2. Sous **Protocole**, sélectionnez **OIDC**.

3. Sélectionnez le **SSO type** dans la liste déroulante.

4. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.

- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre :

- i. Accédez à l'emplacement du certificat de l'autorité de certification.
- ii. Téléchargez le fichier de certificat de l'autorité de certification.

- **N'utilisez pas TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.



Si vous modifiez le certificat de l'autorité de certification, testez immédiatement **"Redémarrez le service mgmt-api sur les nœuds d'administration"** et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

5. Sélectionnez **Continuer**. La page Fournir l'identifiant de la partie de confiance s'affiche.

Étape 2 : Saisissez les informations du client

Remplissez les champs de l'étape « Saisie des informations client » de l'assistant.

Étapes

1. Spécifiez l'**identificateur de la partie de confiance** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque configuration OIDC.
 - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez SG ou StorageGRID.
 - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple, SG-[HOSTNAME]. Inclure cette chaîne génère un tableau affichant la configuration OIDC de chaque nœud d'administration de la grille, en fonction du nom d'hôte du nœud.



Vous devez configurer OIDC pour les nœuds d'administration de votre système StorageGRID. Cela garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration. Vous pouvez utiliser la même configuration OIDC pour tous les nœuds d'administration (recommandé) ou définir une configuration OIDC différente pour chaque nœud d'administration.

2. Saisissez l'**ID client**, le **secret client** et l'**URL du point de terminaison OpenID** pour chaque identifiant de partie de confiance.
3. Sélectionnez **Enregistrer et entrez en mode sandbox**.

Étape 3 : Test de la configuration

Après être passé en mode sandbox, vous pouvez finaliser et tester la configuration du type SSO que vous avez sélectionné.

Le mode sandbox facilite la configuration aller-retour et le test de tous vos paramètres avant d'activer l'authentification unique (SSO). StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, seuls les utilisateurs fédérés et les utilisateurs locaux peuvent se connecter.

Étapes

1. À partir de la page Configurer SSO, recherchez le lien à l'étape Configuration de test de l'assistant.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.

2. Sélectionnez le lien, ou copiez et collez l'URL dans un nouvel onglet pour accéder à la page de connexion de votre fournisseur d'identité.
3. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion et de déconnexion SSO réussissent, une bannière verte apparaît.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Suivez les étapes de l'assistant pour accéder à la page de configuration de test de chaque nœud d'administration de votre grille.
5. Répétez les étapes 2 et 3 pour vérifier la connexion SSO pour chaque nœud d'administration.

Étape 4 : Activez l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à chaque nœud d'administration, vous pouvez activer l'authentification unique (SSO) pour l'ensemble de votre système StorageGRID.



Lorsque l'authentification unique (SSO) est activée, tous les utilisateurs doivent utiliser SSO pour accéder au Grid Manager, au Tenant Manager, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID. StorageGRID ne fournit pas d'exemple de script d'authentification pour tous les fournisseurs SSO pris en charge.

Étapes

1. À partir de l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Consultez le message d'avertissement et sélectionnez **Activer SSO**.

L'authentification unique est désormais activée. La page d'authentification unique s'affiche et inclut désormais les détails du SSO que vous venez de configurer.

3. Pour modifier la configuration, sélectionnez **Modifier**.
4. Pour désactiver l'authentification unique, sélectionnez **Désactiver**.



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 Entra ID, 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).

Configurer l'authentification unique (SSO) avec SAML

Découvrez comment configurer l'authentification unique (SSO) dans StorageGRID à l'aide de SAML

La mise en place de l'authentification unique (SSO) dans StorageGRID permet à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs.

Vous pouvez configurer l'authentification unique (SSO) dans StorageGRID à l'aide d'OpenID Connect (OIDC) ou de SAML. Suivez ces étapes générales pour configurer l'authentification unique dans StorageGRID à l'aide

de SAML ou découvrez ["Configuration de l'authentification unique \(SSO\) à l'aide d'OIDC"](#).

1

Configurer l'authentification unique (SSO)

Sélectionnez l'assistant de configuration SSO pour SAML. Configurez ensuite l'authentification unique avec votre fournisseur d'identité et passez en mode sandbox.

Apprenez-en plus sur ["Configuration de l'authentification unique \(SSO\) à l'aide de SAML"](#)

2

Configurer le fournisseur d'identité

En fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser, vous pouvez sélectionner Active Directory ou Entra ID pour le type de service LDAP de fédération d'identités.

- Pour Active Directory Federation Service (AD FS), vous pouvez utiliser le fournisseur d'identité AD FS, Entra ID ou PingFederate.
- Pour Entra ID, vous ne pouvez utiliser que le fournisseur d'identité Entra ID.

Utilisez le logiciel du fournisseur d'identité SSO pour configurer SAML pour chaque nœud d'administration de votre grille.

- Découvrez ["création d'un groupe d'applications pour chaque nœud d'administration"](#) dans Active Directory
- Découvrez ["création d'une application pour chaque nœud d'administration"](#) dans Entra ID
- Découvrez ["création d'une connexion à un fournisseur de services pour chaque Admin Node"](#) dans PingFederate

3

Configuration de test

Après avoir configuré SAML pour chaque nœud d'administration, retournez à l'assistant de configuration SSO et testez la configuration.

Apprenez-en plus sur ["Test de la configuration pour l'authentification unique \(SSO\)"](#)

4

Activer l'authentification unique (SSO)

Activez l'authentification unique (SSO) pour tous les utilisateurs de StorageGRID.

Apprenez-en plus sur ["Activation de l'authentification unique \(SSO\) pour les utilisateurs de StorageGRID"](#)

Configurer l'authentification unique (SSO) dans StorageGRID à l'aide de SAML

Suivez l'assistant de configuration SSO pour SAML et passez en mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID. Après avoir activé SSO, vous pouvez revenir en mode sandbox si nécessaire pour modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

- Vous avez le "[Autorisation d'accès racine](#)".
- Vous avez configuré la fédération des identités pour votre système StorageGRID.
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Entra ID, en fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Service de fédération Active Directory (AD FS)	• Active Directory • ID d'entrée • PingFederate
ID d'entrée	ID d'entrée

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. Le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour les demandes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Entra ID inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs, vous effectuez les tâches suivantes :

1. Configurer les paramètres dans StorageGRID.
2. Utilisez le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Entra ID) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration.
3. Revenez 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.

Étape 1 : Fournir les détails du fournisseur d'identité

Accédez à l'assistant et complétez les champs de la page Fournir les détails du fournisseur d'identité.

Étapes

1. Accédez à l'assistant :
 - a. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**. La page d'authentification unique apparaît.



Si le bouton Configurer les paramètres SSO est désactivé, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. "[Configuration requise et considérations pour l'authentification unique](#)".

- b. Sélectionnez **Configurer les paramètres SSO**. La page Fournir les détails du fournisseur d'identité s'affiche.
2. Sous **Protocole**, sélectionnez **SAML**.
3. Sélectionnez le **SSO type** dans la liste déroulante.
4. Si vous avez sélectionné Active Directory comme type SSO, 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 à Windows Server Manager. Sélectionnez **Outils > AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

5. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.
 - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
 - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.



Si vous modifiez le certificat de l'autorité de certification, testez immédiatement "[Redémarrez le service mgmt-api sur les nœuds d'administration](#)" et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

6. Sélectionnez **Continuer**. La page Fournir l'identifiant de la partie de confiance s'affiche.

Étape 2 : Fournissez les relations d'approbation de parties de confiance, les applications d'entreprise ou les connexions SP

Remplissez les champs de l'étape 2 de l'assistant en fonction du type de SSO que vous avez sélectionné.

Active Directory

Remplissez les champs de l'étape **Fournir l'identifiant de la partie de confiance**.

Étapes

1. 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 grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
 - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG- [HOSTNAME]` . L'inclusion de cette chaîne génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration dans la grille, en fonction du nom d'hôte du nœud.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

2. Sélectionnez **Enregistrer et entrez en mode sandbox**.

ID d'entrée

Remplissez les champs de l'étape **Configurer les applications d'entreprise**.

Étapes

1. 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 Entra ID.
 - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
 - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG- [HOSTNAME]` . L'inclusion de cette chaîne 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. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

2. Suivez les étapes décrites dans "[Créer des applications d'entreprise dans Entra ID](#)" pour créer une application d'entreprise pour chaque Admin Node répertorié dans le tableau.
3. À partir d'Entra ID, copiez l'URL des métadonnées de la fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ **URL des métadonnées de la fédération** correspondant dans StorageGRID.
4. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer et passer en mode sandbox**.

PingFederate

Remplissez les champs à l'étape **Fournir l'ID de connexion SP**.

Étapes

1. Dans la section SP (Service Provider), spécifiez l'ID de connexion **SP** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.
 - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
 - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]`. L'inclusion de cette chaîne 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. La présence d'une connexion SP pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

2. Spécifiez l'URL des métadonnées de fédération pour chaque nœud d'administration dans le champ **URL des métadonnées de fédération**.

Utilisez le format suivant :

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection  
ID>
```

3. Sélectionnez **Enregistrer et entrez en mode sandbox**.

Étape 3 : Configurez les relations d'approbation des parties de confiance, les applications d'entreprise ou les connexions SP

Après avoir enregistré la configuration et être entré en mode sandbox, vous pouvez terminer et tester la configuration pour le type SSO que vous avez sélectionné.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, seuls les utilisateurs fédérés et les utilisateurs locaux peuvent se connecter.

Active Directory

Étapes

1. Accédez à Active Directory Federation Services (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 Configurer SSO.

Vous devez créer une confiance pour chaque nœud d'administration indiqué dans le tableau.

Pour obtenir des instructions, rendez-vous sur ["Créer des fiducies de tiers de confiance dans AD FS"](#).

ID d'entrée

Étapes

1. Dans la page Single Sign-on du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
 - a. Connectez-vous au nœud.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes décrites ["Créer des applications d'entreprise dans Entra ID"](#) pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Entra ID correspondante.

PingFederate

Étapes

1. Dans la page Single Sign-on du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
 - a. Connectez-vous au nœud.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. ["Créez une ou plusieurs connexions de fournisseur de services pour StorageGRID"](#). Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué dans le tableau de la page Configurer SSO) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

Vous devez créer une connexion SP pour chaque nœud d'administration affiché dans le tableau.

Étape 4 : Tester la configuration

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID, vérifiez 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 Configurer SSO, recherchez le lien à l'étape Configuration de test de l'assistant.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.

2. Sélectionnez le lien ou copiez-collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
3. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez l'identifiant de partie de confiance pour votre nœud d'administration principal et sélectionnez **connexion**.
4. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

ID d'entrée

Étapes

1. Accédez à la page d'identification unique sur le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Depuis la page Configurer SSO, sélectionnez le premier lien dans le message du mode Sandbox.

Sélectionnez et testez un lien à la fois.

2. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
3. Cliquez sur le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si un message page expirée s'affiche, sélectionnez le bouton **Retour** dans votre navigateur et

soumettez à nouveau vos informations d'identification.

Étape 5 : Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à chaque nœud d'administration, vous pouvez activer l'authentification unique (SSO) pour l'ensemble de votre système StorageGRID.



Lorsque l'authentification SSO est activée, tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. À partir de l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Consultez le message d'avertissement et sélectionnez **Activer SSO**.

L'authentification unique est désormais activée. La page d'authentification unique s'affiche et inclut désormais les détails du SSO que vous venez de configurer.

3. Pour modifier la configuration, sélectionnez **Modifier**.
4. Pour désactiver l'authentification unique, sélectionnez **Désactiver l'authentification unique**.



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 Entra ID, 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).

Et ensuite ?

Après avoir configuré l'authentification unique (SSO) à l'aide de SAML, configurez le fournisseur d'identité pour les Admin Nodes.

Si votre fournisseur d'identité est...	Vous devez...
Active Directory	" Créez un groupe d'applications pour chaque nœud d'administration "
ID d'entrée	" Créez une application pour chaque nœud d'administration "
PingFederate	" Créez une connexion de fournisseur de services pour chaque nœud d'administration "

Créer des approbations de parties de confiance dans AD FS pour SAML dans StorageGRID

Vous devez utiliser les services de fédération Active Directory (AD FS) pour créer une approbation de partie de confiance pour chaque nœud d'administration pour SAML dans votre système. Vous pouvez créer des approbations de partie de confiance à l'aide de commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou

en saisissant les données manuellement.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **AD FS** comme type SSO.
- Vous avez "[entré en mode bac à sable](#)" dans Grid Manager.
- 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 Configurer SSO de StorageGRID .



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.
- Si vous créez manuellement la confiance de la partie utilisatrices, vous disposez du certificat personnalisé chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.

Description de la tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Créez une confiance en vous appuyant sur Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties qui font confiance.

Étapes

1. Dans le menu Démarrer de Windows, sélectionnez l'icône PowerShell avec le bouton droit de la souris et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, saisissez la commande suivante :

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Pour *Admin_Node_Identifier*, entrez l'identificateur de partie utilisatrice pour le nœud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple SG-DC1-ADM1, .
- Pour *Admin_Node_FQDN*, entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > AD FS Management**.

L'outil de gestion AD FS s'affiche.

4. Sélectionnez **AD FS > confiance de la partie de confiance**.

La liste des fiduciaires de tiers de confiance s'affiche.

5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :

- a. Recherchez la confiance de la partie de confiance que vous venez de créer.
- b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
- c. Sélectionnez une stratégie de contrôle d'accès.
- d. Sélectionnez **appliquer**, puis **OK**

6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiduciaire de compte comptant :

- a. Recherchez la confiance de la partie de confiance que vous venez de créer.
- b. Cliquez avec le bouton droit de la souris sur la fiduciaire et sélectionnez **Modifier la politique d'émission des sinistres**.
- c. Sélectionnez **Ajouter règle**.
- d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
- e. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

- f. Pour le magasin d'attributs, sélectionnez **Active Directory**.
- g. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
- h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
- i. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
- b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.

8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

9. Une fois que vous avez terminé, retournez sur StorageGRID et "[tester toutes les fiduciaires des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créez une confiance de partie de confiance en vous important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque confiance de fournisseur en accédant aux métadonnées SAML de chaque nœud d'administration.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.
5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

`https://Admin_Node_FQDN/api/saml-metadata`

Pour *Admin_Node_FQDN*, entrez le nom de domaine complet pour le même noeud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

6. Terminez l'assistant confiance de la partie de confiance, enregistrez la confiance de la partie de confiance et fermez l'assistant.



Lors de la saisie du nom d'affichage, utilisez l'identificateur de partie comptant pour le noeud d'administration, exactement comme il apparaît sur la page d'ouverture de session unique dans le Gestionnaire de grille. Par exemple `SG-DC1-ADM1`, .

7. Ajouter une règle de sinistre :
 - a. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
 - b. Sélectionnez **Ajouter règle** :
 - c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
 - d. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.
 - e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - f. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
 - g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
 - h. Sélectionnez **Terminer** et sélectionnez **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

10. Une fois que vous avez terminé, retournez sur StorageGRID "[tester toutes les fiducies des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créer une confiance de partie de confiance manuellement

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement** et sélectionnez **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :

- a. Entrez un nom d'affichage pour ce nœud d'administration.

Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple SG-DC1-ADM1, .

- b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.
- c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.
- d. Saisissez l'URL du noeud final du service SAML pour le noeud d'administration :

`https://Admin_Node_FQDN/api/saml-response`

Pour *Admin_Node_FQDN*, entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

- e. Sur la page configurer les identificateurs, spécifiez l'identificateur de partie de confiance pour le même noeud d'administration :

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, entrez l'identificateur de partie utilisatrice pour le noeud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple SG-DC1-ADM1, .

- f. Vérifiez les paramètres, enregistrez la confiance de la partie utilisatrices et fermez l'assistant.

La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.



Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

6. Pour démarrer l'assistant règle de sinistre, sélectionnez **Ajouter règle** :

a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.

b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

c. Pour le magasin d'attributs, sélectionnez **Active Directory**.

d. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.

e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

f. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :

a. Sélectionnez **Ajouter SAML**.

b. Sélectionnez **Endpoint Type > SAML Logout**.

c. Sélectionnez **Redirect > Redirect**.

d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

`https://Admin_Node_FQDN/api/saml-logout`

Pour *Admin_Node_FQDN*, entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

a. Sélectionnez **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :

a. Ajouter le certificat personnalisé :

- Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
- Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.



L'utilisation du certificat par défaut du nœud d'administration (`server.crt`) n'est pas recommandée. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurerez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

b. Sélectionnez **appliquer**, puis **OK**.

Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

11. Une fois que vous avez terminé, retournez sur StorageGRID "[tester toutes les fiducies des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créez des applications d'entreprise dans Entra ID pour SAML dans StorageGRID

Utilisez Entra ID pour créer une application d'entreprise pour chaque nœud d'administration pour SAML dans votre système.

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Entra ID** comme type d'authentification unique.
- Vous avez "[entré en mode bac à sable](#)" dans Grid Manager.
- 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 Configurer SSO.



Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Entra ID.
- Vous disposez d'un compte Entra ID avec un abonnement actif.
- Vous disposez de l'un des rôles suivants dans le compte Entra ID : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal de service.

Étape 1 : Accédez à Entra ID

Étapes

1. Connectez-vous au "[Portail Azure](#)".
2. Accéder à "[ID d'entrée](#)".
3. Sélectionnez "[Les applications d'entreprise](#)".

Étape 2 : Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Entra ID dans StorageGRID, vous devez utiliser Entra ID pour créer une application d'entreprise pour chaque nœud d'administration. Vous copierez les URL des métadonnées de la fédération depuis Entra ID et les collerez dans les champs **URL des métadonnées de la fédération** correspondants sur la page Configurer SSO.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
 - a. Dans le volet Applications Entra ID Enterprise, sélectionnez **Nouvelle application**.
 - b. Sélectionnez **Créez 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 Configurer SSO.
 - d. Laissez le bouton radio **intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie)** sélectionné.

- e. Sélectionnez **Créer**.
 - f. Sélectionnez le lien **Get Started** dans **2. Configurez la case Single Sign On** ou sélectionnez le lien **Single Sign-on** dans la marge de gauche.
 - g. Sélectionnez la case **SAML**.
 - h. Copiez l'URL **App Federation Metadata URL**, que vous trouverez sous **étape 3 SAML Signing Certificate**.
 - i. Accédez à la page Configurer SSO 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 Configurer SSO.

Étape 3 : Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID.

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.
 - a. Connectez-vous à StorageGRID à partir du nœud d'administration.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
 - d. Enregistrez le fichier que vous téléchargerez dans Entra ID.

Étape 4 : Charger les métadonnées SAML dans chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID, effectuez les étapes suivantes dans Entra ID :

Étapes

1. Revenez au portail Azure.
2. Répétez cette procédure pour chaque application d'entreprise :



Vous devrez peut-être actualiser la page applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

- a. Accédez à la page Propriétés de l'application d'entreprise.
 - b. Définissez **affectation requise** sur **non** (sauf si vous souhaitez configurer séparément les affectations).
 - c. Accédez à la page Single Sign-on.
 - d. Terminez la configuration SAML.
 - e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.
 - f. Une fois le fichier chargé, sélectionnez **Enregistrer**, puis **X** pour fermer le volet. Vous revenez à la page configurer un Single Sign-on avec SAML.
3. ["Tester chaque application"](#).

Créez des connexions de fournisseur de services dans PingFederate pour SAML dans StorageGRID

Utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration pour SAML dans 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 sélectionné **Ping Federate** comme type SSO.
- Vous avez ["entré en mode bac à sable"](#) dans Grid Manager.
- 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 Configurer SSO.
- Vous avez téléchargé les métadonnées **SAML** pour chaque nœud d'administration de votre système.
- Vous avez l'expérience de la création de connexions SP dans PingFederate Server.
- Vous avez le ["Guide de référence de l'administrateur"](#) serveur for PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous avez le ["Autorisation d'administrateur"](#) pour le serveur PingFederate.

Description de la tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées sur votre version.

Remplir les conditions préalables dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lors de la configuration des connexions du processeur de service.

Créer un magasin de données

Si ce n'est pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées ["configuration de la fédération des identités"](#) dans StorageGRID.

- **Type:** Répertoire (LDAP)
- **Type LDAP :** Active Directory
- **Nom d'attribut binaire :** saisissez **objectGUID** dans l'onglet attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

- **Type:** LDAP Nom d'utilisateur Mot de passe validateur des informations d'identification
- **Magasin de données :** sélectionnez le magasin de données que vous avez créé.
- **Base de recherche :** saisissez des informations à partir de LDAP (par exemple, DC=saml,DC=sgws).

- **Filtre de recherche** : sAMAccountName=\${username}
- **Portée** : sous-arbre

Créer une instance d'adaptateur IDP

Si ce n'est déjà fait, créez une instance de carte IDP.

Étapes

1. Accédez à **Authentication > Integration > IDP Adapters**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IDP adapter**.
4. Dans l'onglet carte IDP, sélectionnez **Ajouter une nouvelle ligne à 'Validators Credentials'**.
5. Sélectionnez le [validateur des informations d'identification du mot de passe](#) tu as créé.
6. Dans l'onglet attributs de l'adaptateur, sélectionnez l'attribut **nom d'utilisateur** pour **pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **sécurité > clés de signature et de déchiffrement**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML téléchargées depuis StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient la plupart des valeurs spécifiques dont vous avez besoin.



Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID afin que les utilisateurs puissent se connecter en toute sécurité à n'importe quel nœud et en dehors. Suivez ces instructions pour créer la première connexion du processeur de service. Ensuite, accédez à [Créer des connexions SP supplémentaires](#) pour créer les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **applications > intégration > connexions SP**.
2. Sélectionnez **Créer connexion**.
3. Sélectionnez **ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Browser SSO Profiles** et **SAML 2.0** comme protocole.

Importation des métadonnées SP

Étapes

1. Dans l'onglet Importer les métadonnées, sélectionnez **fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page Configurer SSO pour le nœud d'administration.
3. Passez en revue le résumé des métadonnées et les informations fournies dans l'onglet Infos générales.

L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion SP StorageGRID. (Par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'adresse IP du nœud d'administration StorageGRID.

4. Sélectionnez **Suivant**.

Configurer SSO du navigateur IDP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **configurer SSO du navigateur**.
2. Dans l'onglet des profils SAML, sélectionnez les options **SSO** initiée par le SP, **SLO initial du SP**, **SSO initié par l'IDP** et **SLO** lancé par l'IDP.
3. Sélectionnez **Suivant**.
4. Dans l'onglet durée de vie de l'assertion, n'apportez aucune modification.
5. Dans l'onglet création d'assertion, sélectionnez **configurer la création d'assertion**.
 - a. Dans l'onglet mappage d'identité, sélectionnez **Standard**.
 - b. Dans l'onglet Contrat d'attribut, utilisez **SAML_SUBJECT** comme Contrat d'attribut et le format de nom non spécifié qui a été importé.
6. Pour prolonger le contrat, sélectionnez **Supprimer** pour supprimer le `urn:oid`, qui n'est pas utilisé.

Mapper l'instance de l'adaptateur

Étapes

1. Dans l'onglet mappage de la source d'authentification, sélectionnez **mappage d'une nouvelle instance de carte**.
2. Dans l'onglet instance d'adaptateur, sélectionnez le **instance d'adaptateur** que vous avez créé.
3. Dans l'onglet méthode de mappage, sélectionnez **récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Data Store, indiquez une description et sélectionnez le **magasin de données** que vous avez ajouté.
6. Dans l'onglet LDAP Directory Search :
 - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
 - Pour l'étendue de la recherche, sélectionnez **sous-arbre**.
 - Pour la classe d'objets racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet types d'encodage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet filtre LDAP, entrez **sAMAccountName=\${username}**.

9. Dans l'onglet 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 et enregistrez la source d'attribut.
11. Dans l'onglet Source de l'attribut FailSave, sélectionnez **abandonner la transaction SSO**.
12. Passez en revue le résumé et sélectionnez **Done**.
13. Sélectionnez **Done**.

Configurer les paramètres de protocole

Étapes

1. Dans l'onglet **connexion SP > connexion du navigateur SSO > Paramètres de protocole**, sélectionnez **configurer les paramètres de protocole**.
2. Dans l'onglet URL du service d'utilisateur d'assertion, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**POST** pour la liaison et `/api/saml-response` pour l'URL du point final).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du noeud final).
4. Dans l'onglet Allowable SAML Bindings, désactivez **ARTEFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases **exiger la signature des requêtes Authn** et **toujours signer l'assertion** cochées.
6. Dans l'onglet Stratégie de cryptage, sélectionnez **aucun**.
7. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres SSO du navigateur.

Configurer les informations d'identification

Étapes

1. Dans l'onglet connexion SP, sélectionnez **informations d'identification**.
2. Dans l'onglet informations d'identification, sélectionnez **configurer les informations d'identification**.
3. Sélectionnez le [signature du certificat](#) vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **gérer les paramètres de vérification de signature**.
 - a. Dans l'onglet modèle de confiance, sélectionnez **non ancré**.
 - b. Dans l'onglet certificat de vérification de signature, vérifiez les informations de certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Passez en revue les écrans de résumé et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion du processeur de service pour créer les connexions du processeur de service dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.



Les connexions SP des différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de signature, Et l'URL de réponse SLO.

Étapes

1. Sélectionnez **action** > **copie** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Entrez l'ID de connexion et le nom de connexion de la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
 - a. Sélectionnez **action** > **mettre à jour avec métadonnées**.
 - b. Sélectionnez **Choisissez fichier** et chargez les métadonnées.
 - c. Sélectionnez **Suivant**.
 - d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur en raison de l'attribut inutilisé :
 - a. Sélectionnez la nouvelle connexion.
 - b. Sélectionnez **configurer le navigateur SSO** > **configurer la création d'assertion** > **Contrat d'attribut**.
 - c. Supprimez l'entrée pour **urn:oid**.
 - d. Sélectionnez **Enregistrer**.

Désactiver SSO dans StorageGRID

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération des identités.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**.

La page authentification unique s'affiche.

2. Sélectionnez **Désactiver**.
3. Sélectionnez **Oui**.

Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.

La prochaine fois que vous vous connectez à StorageGRID, la page de connexion StorageGRID s'affiche et vous devez entrer le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique (SSO) pour un nœud d'administration StorageGRID

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez le mot de passe de l'utilisateur racine local.

Description de la tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter à Grid Manager en tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.



La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case **Activer SSO** de la page ouverture de session unique du gestionnaire de grille reste cochée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. En fonction de votre configuration SSO, exécutez l'une des commandes suivantes :

SAML

```
disable-saml
```

OIDC

```
disable-oidc
```

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver l'authentification SSO.

Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

La page de connexion à Grid Manager s'affiche car SSO a été désactivé.

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :
 - a. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - b. Modifiez les paramètres SSO incorrects ou obsolètes.
 - c. Sélectionnez **Enregistrer**.

La sélection de **Enregistrer** sur la page ouverture de session unique permet de réactiver automatiquement SSO pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :
 - a. Effectuez les tâches que vous souhaitez effectuer.
 - b. Sélectionnez **se déconnecter** et fermez le Gestionnaire de grille.
 - c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :
 - Exécutez la commande suivante : `enable-saml`

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

Confirmez que vous souhaitez activer le SSO.

Un message indique que l'authentification unique est activée sur le nœud.

- Redémarrer le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Utilisez la vérification multi-administrateurs

Découvrez la vérification multi-administrateur de StorageGRID

En tant qu'administrateur StorageGRID, vous pouvez utiliser la vérification multi-administrateurs (MAV) pour garantir que certaines opérations ne peuvent être effectuées qu'après approbation des administrateurs désignés. La MAV contribue à prévenir les modifications accidentelles ou non autorisées de votre système StorageGRID.

MAV est désactivé par défaut.

Aperçu de la configuration MAV

Pour configurer MAV, vous devrez effectuer les tâches suivantes :

- Créez un ou plusieurs groupes d'administrateurs. Les administrateurs MAV disposent d'un droit d'approbation et de veto.
- Activez la fonctionnalité de vérification multi-administrateur.

- Sélectionnez parmi un ensemble d'opérations protégées.

Un utilisateur doit disposer des droits d'accès Root pour effectuer la configuration initiale et apporter des modifications ultérieurement.

Comment les opérations protégées sont gérées dans le cadre du MAV

Lorsque MAV est activé, l'exécution de chaque opération protégée nécessite les étapes suivantes :

1. Lorsqu'un utilisateur lance l'opération, une requête est générée.
2. Avant que l'opération puisse être effectuée, au moins un administrateur MAV doit approuver.
3. Une fois approuvée, l'opération protégée par MAV est effectuée automatiquement.

Configurer la vérification multi-administrateur StorageGRID

La configuration d'un système de vérification multi-administrateur (MAV) StorageGRID implique la création et la gestion de groupes et d'utilisateurs d'administrateurs MAV, l'activation de la fonction MAV et la sélection ou la configuration des opérations protégées.

Les administrateurs du MAV ont le pouvoir d'approuver et de veto sur les opérations protégées.

Avant de commencer

- Vous avez le ["Autorisation d'accès racine"](#).
- Vous êtes connecté au Grid Manager depuis le nœud d'administration principal.

Étape 1 : Créez des groupes d'administrateurs et des utilisateurs MAV

Vous pouvez ajouter des administrateurs existants à un groupe MAV ou créer de nouveaux administrateurs.

Vous pouvez configurer des utilisateurs Active Directory (AD) en tant qu'administrateurs MAV. L'utilisateur AD doit être configuré en tant qu'administrateur StorageGRID.

Étapes

1. Pour créer un groupe d'administrateurs MAV, suivez les étapes pour ["créer un groupe local ou fédéré"](#).
2. Pour les autorisations de groupe, sélectionnez **Accès racine** ou **Demandes de vérification multi-administrateur**.
3. Ajoutez des utilisateurs locaux ou fédérés au groupe, ou créez de nouveaux utilisateurs locaux et ajoutez-les au groupe en suivant les étapes pour ["créer un utilisateur local"](#).

Étape 2 : Activer ou désactiver MAV

Vous devez activer explicitement la vérification multi-administrateurs (MAV). Si la MAV est activée et que vous décidez de la désactiver alors que des requêtes MAV sont en attente, une notification indique que les requêtes en attente seront supprimées.

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Vérification multi-administrateur > Paramètres MAV**.
2. Cochez la case **Activer MAV** pour activer la vérification multi-administrateur.

3. La section « Groupes d'approbateurs » répertorie les groupes d'administrateurs MAV et les approbateurs.
4. Dans la section Opérations, cochez les cases correspondant aux opérations que vous souhaitez protéger avec MAV.
5. (Facultatif) Si vous souhaitez utiliser les notifications par e-mail pour alerter les administrateurs MAV des demandes d'approbation en attente :
 - a. Si vous n'avez pas configuré de serveur de messagerie, suivez les étapes pour "[configurer un serveur de messagerie](#)".
 - b. Saisissez l'adresse e-mail de l'expéditeur.
 - c. Saisissez un ou plusieurs destinataires pour les notifications par e-mail.
6. Sélectionnez **Enregistrer** pour enregistrer vos modifications.



Si vous choisissez de ne pas configurer les notifications par e-mail, les administrateurs MAV peuvent consulter le tableau de bord du Grid Manager ou vérifier la file d'attente des demandes d'approbation en attente. Pour vérifier la file d'attente des demandes d'approbation, sélectionnez **Other requests** sur la page Multi-admin verification.

Étape 3 : Gérer les opérations protégées

Une fois la vérification multi-administrateur activée, vous pouvez gérer les opérations protégées en cochant ou décochant les cases correspondant aux opérations que vous souhaitez protéger avec MAV.



Pour StorageGRID 12.1, la seule opération protégée est l'activation de la politique ILM. Vous devez cocher la case pour l'activation de la politique ILM si vous souhaitez activer MAV.

Une requête MAV peut avoir l'un des statuts suivants :

- **En attente.** La demande a été initiée.
- **Expiré.** La demande n'a pas été traitée dans les 30 jours. Ou un utilisateur disposant des droits d'accès Root a désactivé MAV, ce qui signifie que toutes les demandes en attente sont expirées.
- **Retiré.** Un utilisateur a retiré sa demande.
- **Approuvé.** Un administrateur MAV a approuvé la demande en attente.
- **Rejeté.** Un administrateur MAV a rejeté la requête en attente.

Résolvez les problèmes de notifications par e-mail MAV

Si les administrateurs MAV ne reçoivent pas de notifications par e-mail concernant les demandes en attente, suivez les étapes suivantes pour résoudre le problème.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".

Étapes

1. Vérifiez vos paramètres.
 - a. Sélectionnez **Configuration > Surveillance > Serveur de messagerie**.
 - b. Vérifiez que les paramètres du serveur de messagerie (SMTP) sont corrects.

- c. Vérifiez que vous avez spécifié des adresses e-mail valides pour les destinataires.
2. Vérifiez votre filtre de spam et assurez-vous que l'e-mail n'a pas été envoyé à un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails de l'adresse de l'expéditeur ne sont pas bloqués.
4. Collectez un fichier journal pour le nœud d'administration, puis contactez le support technique.

Le support technique peut utiliser les informations contenues dans les journaux pour vous aider à déterminer ce qui s'est mal passé. Par exemple, le fichier `prometheus.log` peut afficher une erreur lors de la connexion au serveur spécifié.

Voir "[Collecte de fichiers journaux et de données système](#)".

Demande d'autorisation pour les opérations protégées par MAV dans StorageGRID

En tant qu'administrateur ou utilisateur de StorageGRID, lorsque vous lancez une opération protégée par MAV dans StorageGRID, une demande est générée automatiquement. Un message vous informe que l'opération nécessite une approbation.

Le système StorageGRID définit les opérations protégées par MAV. Lorsque vous initiez une opération protégée par MAV, la requête est envoyée aux administrateurs MAV pour approbation.

Étapes

Le système StorageGRID vous informe que vous avez lancé une opération protégée par MAV.

1. Au besoin, effectuez l'une des tâches suivantes :
 - a. Vérifiez l'état de votre demande en sélectionnant **Configuration > Contrôle d'accès > Vérification multi-administrateur > Mes demandes**.
 - **En attente**. La demande a été initiée.
 - **Expiré**. La demande n'a pas été traitée dans les 30 jours. Ou un utilisateur disposant des droits d'accès Root a désactivé MAV, ce qui signifie que toutes les demandes en attente sont expirées.
 - **Retiré**. Un utilisateur a retiré sa demande.
 - **Approuvé**. Un administrateur MAV a approuvé la demande en attente.
 - **Rejeté**. Un administrateur MAV a rejeté la requête en attente.
 - b. Consultez les demandes en attente des autres utilisateurs en sélectionnant **Configuration > Contrôle d'accès > Vérification multi-administrateur > Autres demandes**.
 - c. Pour annuler une opération, sélectionnez **Mes demandes > la demande que vous souhaitez annuler > Retirer**.

Une fois la demande approuvée par un administrateur MAV, l'opération est effectuée automatiquement.

Si votre demande est rejetée, l'opération n'est pas effectuée et vous pouvez soumettre une nouvelle demande si nécessaire.

Gérer les demandes d'opérations protégées par MAV dans StorageGRID

En tant qu'administrateur MAV, vous pouvez gérer les demandes d'opérations protégées par MAV dans StorageGRID. Vous pouvez consulter vos propres demandes ou celles d'autres utilisateurs en attente, approuver ou refuser des demandes, et consulter

l'historique des demandes précédentes.

Avant de commencer

- Vous appartenez à un groupe d'administrateurs MAV et vous avez le "[Autorisation d'accès racine](#)".
- Vous êtes connecté au Grid Manager depuis le nœud d'administration principal.

Étapes

1. Si vous recevez une notification par e-mail concernant une demande MAV, sélectionnez **Configuration** > **Vérification multi-administrateur** > **Autres demandes**.

De plus, le tableau de bord du Grid Manager affiche une notification pour les demandes MAV en attente.

2. Sélectionnez le bouton radio correspondant à chaque requête que vous souhaitez gérer.
3. Sélectionnez **Approuver** ou **Rejeter** pour approuver ou rejeter les demandes sélectionnées.
4. Pour consulter l'historique des demandes précédentes, sélectionnez **Historique**.

Utiliser la fédération de grille

Découvrez la fédération de grilles StorageGRID

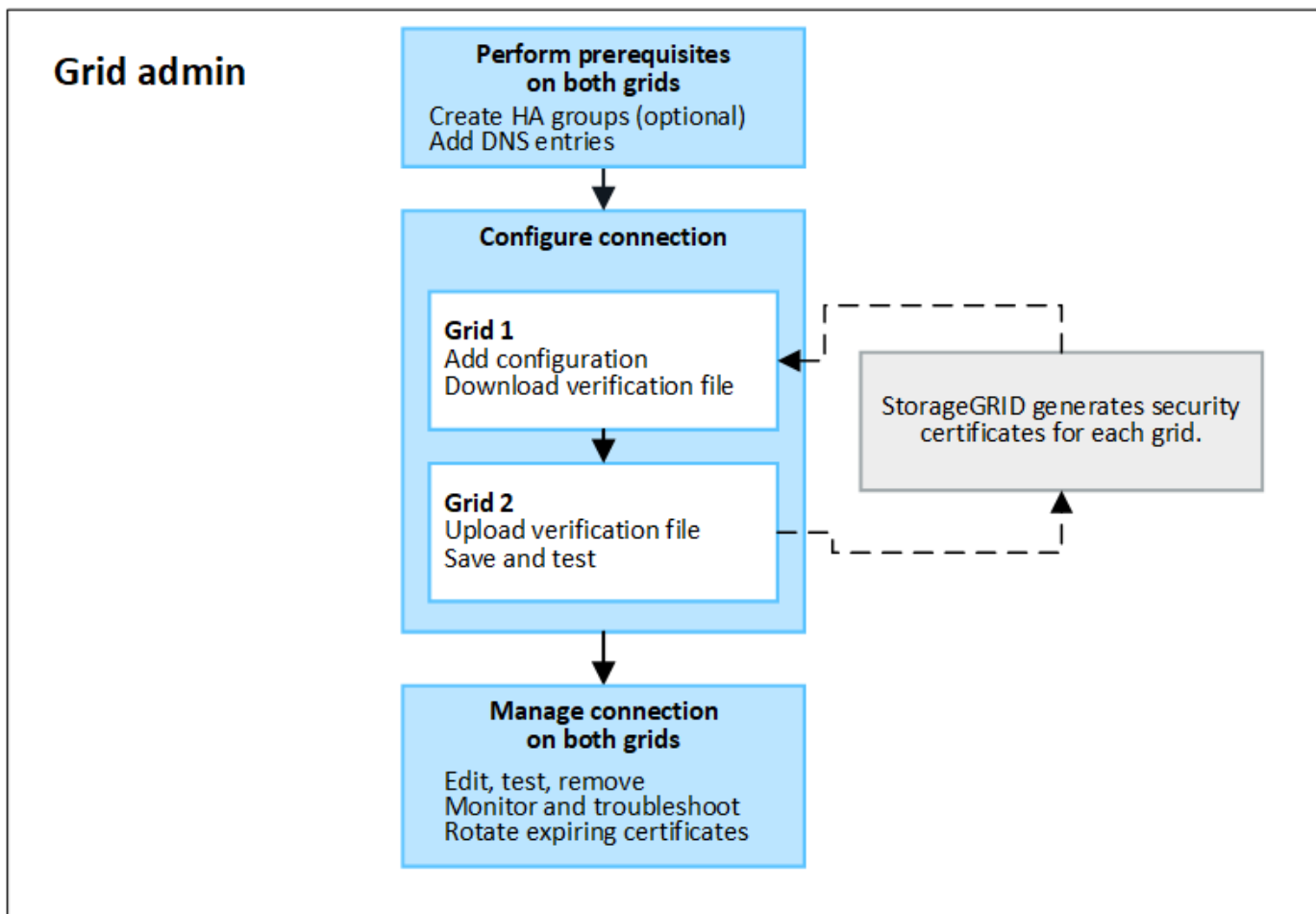
Vous pouvez utiliser la fédération de grilles pour synchroniser les locataires et répliquer leurs objets entre plusieurs systèmes StorageGRID à des fins de reprise après sinistre.

Qu'est-ce qu'une connexion de fédération de grille ?

Une connexion de fédération grid est une connexion bidirectionnelle, fiable et sécurisée entre les nœuds d'administration et de passerelle dans deux systèmes StorageGRID.

Flux de travail pour la fédération de grille

Le diagramme de flux de travail récapitule les étapes de configuration d'une connexion de fédération de grille entre deux grilles.



Considérations et conditions requises pour les connexions de fédération de grille

- Les grilles utilisées pour la fédération de grille doivent exécuter des versions StorageGRID identiques ou ne doivent pas avoir plus d'une différence de version majeure entre elles.

Pour plus de détails sur les exigences de version, consultez ["Notes de mise à jour"](#). Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

- Une grille peut avoir une ou plusieurs connexions de fédération de grille à d'autres grilles. Chaque connexion de fédération de grille est indépendante des autres connexions. Par exemple, si la grille 1 a une connexion avec la grille 2 et une seconde connexion avec la grille 3, il n'y a pas de connexion implicite entre la grille 2 et la grille 3.
- Les connexions de fédération de grille sont bidirectionnelles. Une fois la connexion établie, vous pouvez surveiller et gérer la connexion à partir de l'une ou l'autre grille.
- Au moins une connexion de fédération de grille doit exister avant que vous puissiez utiliser ["synchronisation des comptes"](#) ou ["réplication entre plusieurs grilles"](#).

Exigences en matière de mise en réseau et d'adresse IP

- Les connexions de fédération de grille peuvent se produire sur le réseau de grille, le réseau d'administration ou le réseau client.
- Une connexion de fédération de grille connecte une grille à une autre grille. La configuration de chaque grille spécifie un point de terminaison de fédération grid sur l'autre grille composé de nœuds d'administration, de nœuds de passerelle ou des deux.

- Il est recommandé de connecter les "**Groupe haute disponibilité (HA)**" nœuds de passerelle et d'administration sur chaque grid. L'utilisation des groupes haute disponibilité permet de s'assurer que les connexions de fédération du grid resteront en ligne si les nœuds ne sont plus disponibles. En cas de défaillance de l'interface active de l'un ou l'autre groupe haute disponibilité, la connexion peut utiliser une interface de sauvegarde.
- Il n'est pas recommandé de créer une connexion de fédération de grille qui utilise l'adresse IP d'un nœud d'administration ou d'un nœud de passerelle unique. Si le nœud devient indisponible, la connexion de fédération de grille devient également indisponible.
- "**Réplication entre plusieurs grilles**" D'objets exige que les nœuds de stockage de chaque grid puissent accéder aux nœuds d'administration et de passerelle configurés sur l'autre grid. Pour chaque grid, vérifiez que tous les nœuds de stockage disposent d'une route à large bande passante vers en tant que nœuds d'administration ou nœuds de passerelle utilisés pour la connexion.

Utilisez des FQDN pour équilibrer la charge de la connexion

Pour un environnement de production, utilisez des noms de domaine complets (FQDN) pour identifier chaque grille de la connexion. Créez ensuite les entrées DNS appropriées, comme suit :

- Le nom de domaine complet de la grille 1 est mappé à une ou plusieurs adresses IP virtuelles (VIP) pour les groupes haute disponibilité de la grille 1 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle de la grille 1.
- Le nom de domaine complet de la grille 2 est mappé à une ou plusieurs adresses VIP pour la grille 2 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle dans la grille 2.

Lorsque vous utilisez plusieurs entrées DNS, les demandes d'utilisation de la connexion sont équilibrées de la manière suivante :

- Les entrées DNS qui correspondent aux adresses VIP de plusieurs groupes haute disponibilité sont équilibrées de charge entre les nœuds actifs des groupes haute disponibilité.
- Les entrées DNS qui correspondent aux adresses IP de plusieurs nœuds d'administration ou nœuds de passerelle sont équilibrées de charge entre les nœuds mappés.

Configuration requise pour les ports

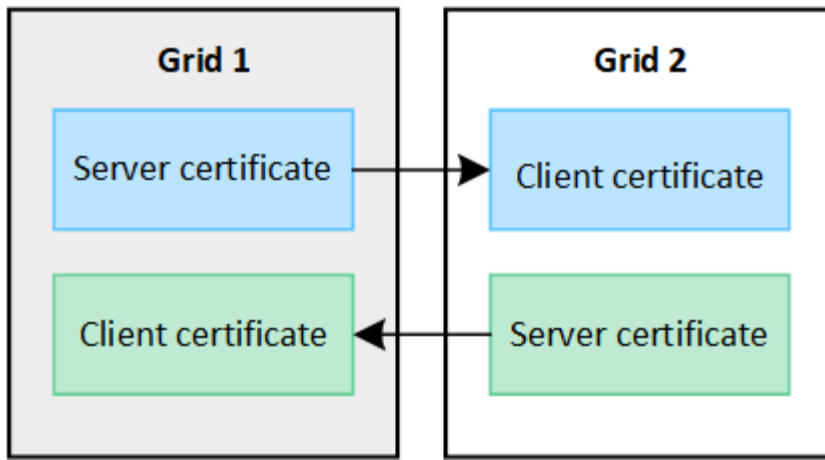
Lors de la création d'une connexion de fédération de grille, vous pouvez spécifier tout numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port.

Vous devez vous assurer qu'aucun nœud d'une grille n'utilise ce port pour d'autres connexions.

Exigences en matière de certificat

Lorsque vous configurez une connexion de fédération de grille, StorageGRID génère automatiquement quatre certificats SSL :

- Certificats de serveur et de client pour authentifier et crypter les informations envoyées de la grille 1 à la grille 2
- Certificats de serveur et de client pour authentifier et crypter les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valides pendant 730 jours (2 ans). Lorsque ces certificats sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats, ce que vous pouvez faire à l'aide de Grid Manager.



Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner. La réplication des données sera en attente jusqu'à la mise à jour des certificats.

En savoir plus >>

- ["Créer des connexions de fédération de grille"](#)
- ["Gérer les connexions de fédération de grille"](#)
- ["Dépanner les erreurs de fédération de grille"](#)

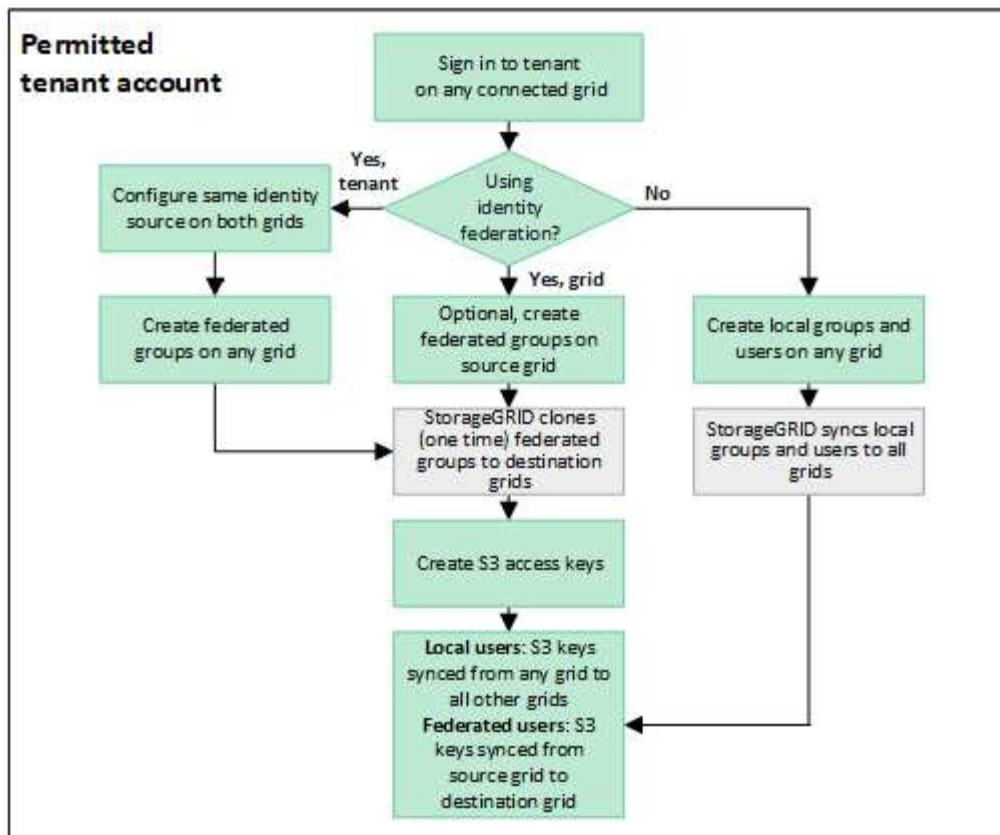
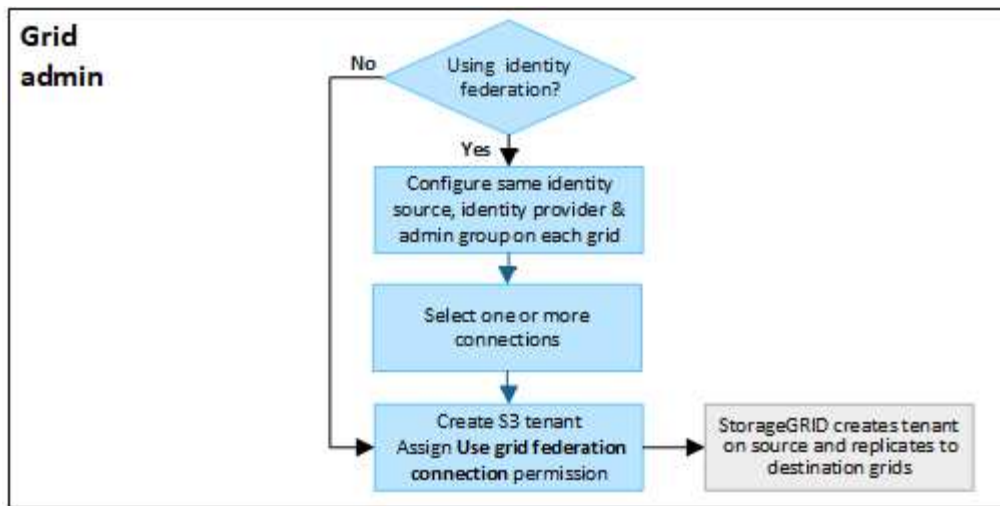
Découvrez la synchronisation des comptes dans StorageGRID

La synchronisation des comptes est la réplication automatique et continue d'un compte locataire, de groupes de locataires, d'utilisateurs locataires et, éventuellement, de clés d'accès S3 entre les systèmes StorageGRID dans un ou plusieurs ["connexions de fédération de grille"](#).

La synchronisation des comptes est requise pour ["réplication entre plusieurs grilles"](#). La synchronisation des informations de compte entre les systèmes StorageGRID garantit que les utilisateurs et les groupes locataires peuvent accéder aux compartiments et aux objets correspondants sur n'importe quelle grille connectée.

Flux de travail pour la synchronisation des comptes

Le diagramme de flux de travail illustre les étapes que les administrateurs de grille et les locataires autorisés devront suivre pour configurer la synchronisation des comptes. Ces étapes sont effectuées après le ["la connexion de fédération de grille est configurée"](#).



Workflow d'administration du grid

Les étapes que les administrateurs du grid effectuent dépendent du type d'authentification unique (SSO) ou de fédération des identités des systèmes StorageGRID "[connexion de fédération de grille](#)".

Configurer l'authentification unique pour la synchronisation des comptes (facultatif)

Si l'un des systèmes StorageGRID de la connexion de fédération de grille utilise SSO, les deux grilles doivent utiliser SSO. Avant de créer les comptes de tenant pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez le même référentiel d'identité pour les deux grilles. Voir "[Utiliser la fédération des identités](#)".

2. Configurez le même fournisseur d'identité SSO (IdP) pour les deux grilles. Voir ["Configurer l'authentification unique"](#).
3. ["Créez le même groupe d'administration"](#) sur les deux grilles en important le même groupe fédéré.

Lorsque vous créez le tenant, vous sélectionnez ce groupe pour obtenir l'autorisation d'accès racine initiale pour les comptes de tenant source et de destination.



Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

Configurer la fédération d'identités au niveau de la grille pour la synchronisation des comptes (facultatif)

Si l'un ou l'autre des systèmes StorageGRID utilise la fédération des identités sans SSO, les deux grilles doivent utiliser la fédération des identités. Avant de créer les comptes de tenant pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez le même référentiel d'identité pour les deux grilles. Voir ["Utiliser la fédération des identités"](#).
2. Si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes de tenant source et de destination, ["créez le même groupe d'administration"](#) sur les deux grilles en important le même groupe fédéré.



Si vous attribuez l'autorisation d'accès racine à un groupe fédéré qui n'existe pas sur les deux grilles, le tenant n'est pas répliqué sur la grille de destination.

3. Si vous ne souhaitez pas qu'un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur root local.

Créez un compte de locataire S3 autorisé

Après avoir configuré éventuellement une SSO ou une fédération d'identités, un administrateur du grid effectue ces étapes pour déterminer quels locataires peuvent répliquer des objets de compartiment vers d'autres systèmes StorageGRID.

Étapes

1. Déterminez la grille que vous souhaitez utiliser comme grille source du locataire pour les opérations de synchronisation des comptes.

La grille dans laquelle le locataire est créé à l'origine est appelée *grille source* du locataire. La grille dans laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

2. Dans cette grille, créez un compte de locataire S3 ou modifiez un compte existant.
3. Attribuez l'autorisation **utiliser la connexion de fédération de grille**.
4. Si le compte de tenant gère ses propres utilisateurs fédérés, attribuez l'autorisation **utiliser son propre référentiel d'identité**.

Si cette autorisation est accordée, les comptes des locataires 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 être synchronisés avec le locataire de destination que si les deux grids utilisent la même source d'identité.

5. Sélectionnez une connexion de fédération de grille spécifique.
6. Enregistrez le nouveau locataire ou le locataire modifié.

Lorsqu'un nouveau locataire avec l'autorisation **utiliser la connexion de fédération de grille** est enregistré, StorageGRID crée automatiquement une réplique de ce locataire sur l'autre grille, comme suit :

- Les deux comptes de tenant possèdent les mêmes ID de compte, nom, quota de stockage et autorisations attribuées.
- Si vous avez sélectionné un groupe fédéré disposant des droits d'accès Root pour le locataire, ce groupe est cloné dans le locataire de destination. Cependant, la synchronisation continue ne s'applique pas aux groupes et utilisateurs fédérés. Seul un clonage ponctuel a lieu.
- Si vous avez sélectionné un utilisateur local pour disposer des droits d'accès Root pour le locataire, cet utilisateur est synchronisé avec le locataire de destination.

Pour plus de détails, consultez ["Gestion des locataires autorisés pour la fédération dans le grid"](#).

Workflow de compte de locataire autorisé

Après qu'un locataire disposant de l'autorisation **Use grid federation connection** a été répliqué sur la grille de destination, les comptes de locataires autorisés peuvent effectuer ces étapes pour synchroniser les groupes de locataires, les utilisateurs et les clés d'accès S3.

Étapes

1. Connectez-vous au compte locataire sur n'importe quelle grille connectée.
2. Si cela est autorisé, configurez la fédération d'identité sur les comptes locataires source et de destination.
3. Créez des groupes et des utilisateurs sur n'importe quelle grille connectée.

Lorsque de nouveaux groupes ou utilisateurs sont créés sur un locataire, StorageGRID les synchronise automatiquement avec le locataire de destination.

4. Création de clés d'accès S3
5. Vous pouvez également synchroniser les clés d'accès S3 du locataire source vers le locataire de destination.

Pour plus de détails sur le flux de travail des comptes locataires autorisés et pour savoir comment les groupes, les utilisateurs et les clés d'accès S3 sont synchronisés, reportez-vous à ["Synchroniser les groupes de locataires et les utilisateurs"](#).

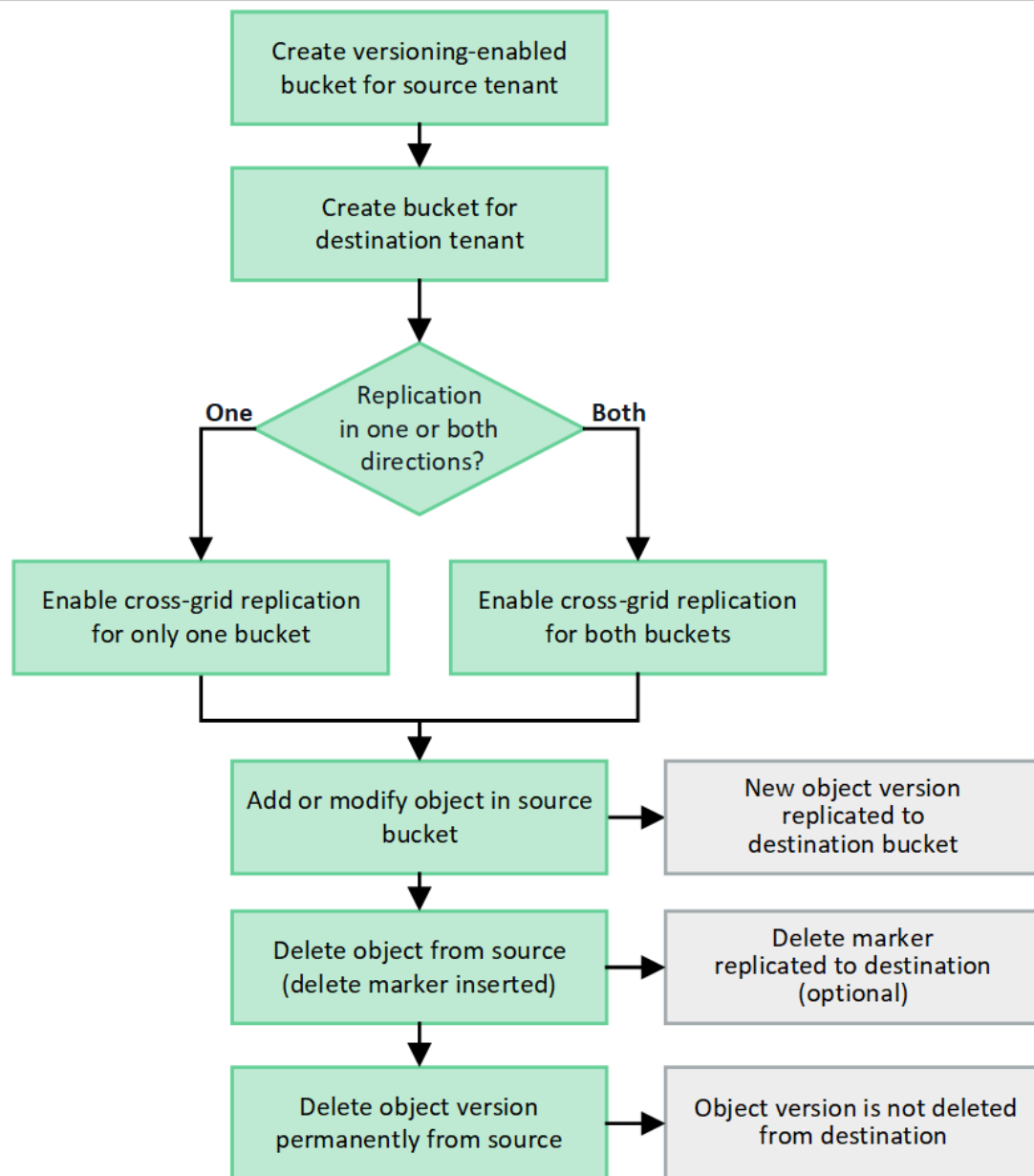
Découvrez la réplication inter-grilles dans StorageGRID

La réplication inter-grilles est la réplication automatique d'objets entre des compartiments S3 sélectionnés dans deux systèmes StorageGRID connectés dans un ["connexion de fédération de grille"](#). ["Synchronisation des comptes"](#) est requis pour la réplication inter-grilles.

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail résume les étapes de configuration de la réplication inter-grille entre les buckets sur deux grilles.

Tenant user



Conditions requises pour la réplication entre les grilles

Si un compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** pour utiliser une ou plusieurs "[connexions de fédération de grille](#)", un utilisateur locataire disposant de l'autorisation d'accès Root peut créer des compartiments (« source » et « destination ») dans les comptes locataires correspondants sur chaque grille. Ces compartiments :

- Peuvent avoir des noms différents les uns des autres
- Peut avoir différentes régions
- La gestion des versions doit être activée
- Doit disposer de l'une des configurations de verrouillage d'objet S3 suivantes :
 - source : **désactivé**, destination : **désactivé**
 - source : **activée**, destination : **activée**

- source : **désactivé**, destination : **activé**

Une fois que vous avez créé les deux compartiments, vous pouvez configurer la réplication inter-grilles pour l'un ou les deux compartiments.

En savoir plus >>

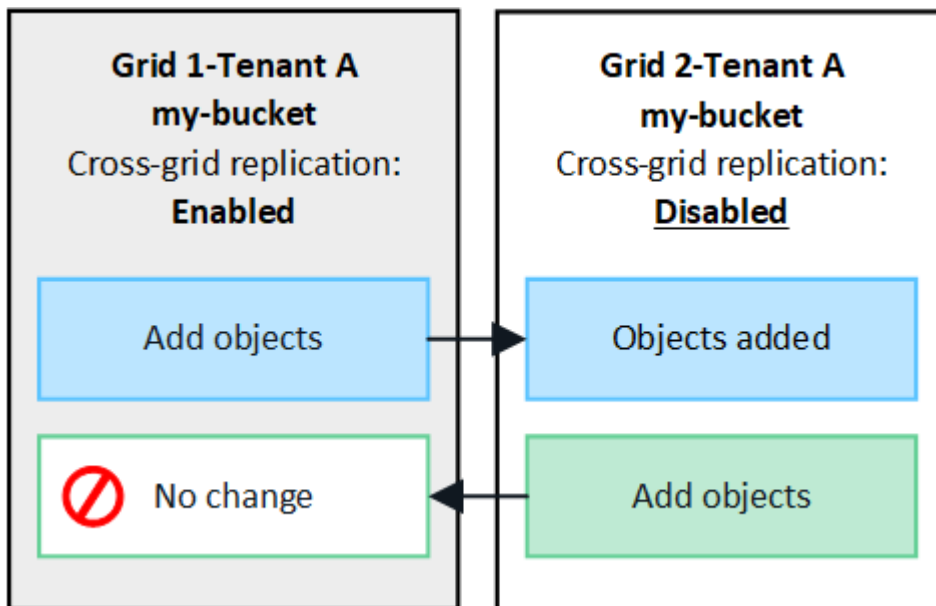
["Gérer la réplication entre les grilles"](#)

Fonctionnement de la réplication entre les grilles

Vous pouvez configurer la réplication inter-grille pour qu'elle se produise dans un sens ou dans les deux sens.

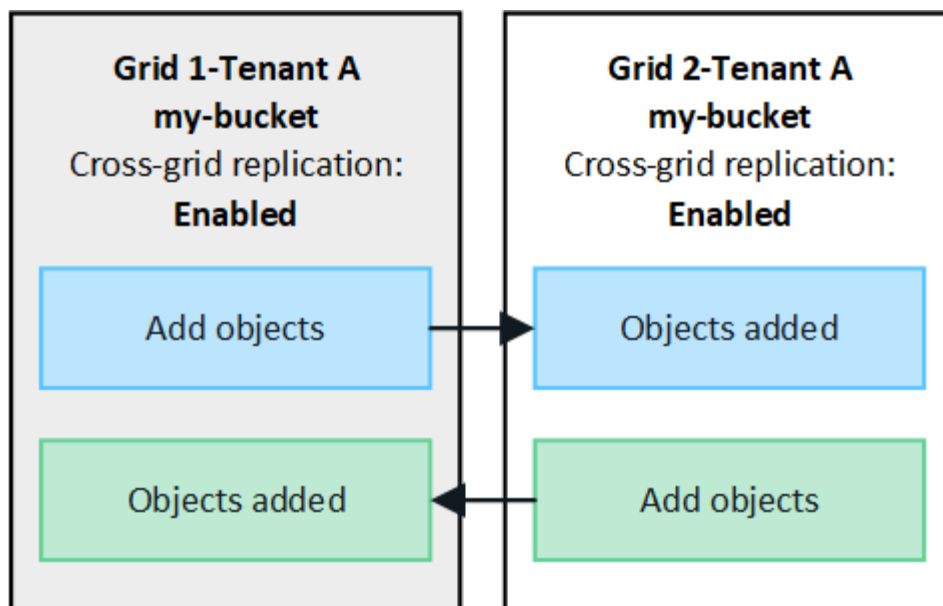
Réplication dans une direction

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 ce n'est pas activé dans l'autre sens.



Réplication dans les deux sens

Si vous activez la réplication inter-grid pour le même compartiment sur les deux grilles, les objets ajoutés à l'un des compartiments sont répliqués sur l'autre grille. Dans la figure, la réplication inter-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 compartiment pour lequel la réplication inter-grille est activée, les événements suivants se produisent :

1. StorageGRID réplique automatiquement l'objet depuis le compartiment source vers le compartiment de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, dont le nombre d'autres opérations de réplication en attente.

Le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête `GetObject` ou `HeadObject`. La réponse inclut un `StorageGRID` spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui a l'une des valeurs suivantes :

Grille	État de la réplication
Source	• TERMINÉ : la réplication a réussi pour toutes les connexions de grille. • EN ATTENTE : l'objet n'a pas été répliqué vers au moins une connexion de grille. • ÉCHEC : La réplication n'est 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 règles ILM actives de chaque grille pour gérer les objets, comme n'importe quel autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservé indéfiniment, tandis que la copie de l'objet A répliqué sur la grille 2 peut être stockée avec un code d'effacement 2+1 et supprimée après trois ans.

Que se passe-t-il lorsque des objets sont supprimés ?

Comme décrit dans ["Supprimer le flux de données"](#), StorageGRID peut supprimer un objet pour l'une des raisons suivantes :

- Le client S3 émet une demande de suppression.
- Un utilisateur tenant Manager sélectionne l'["Supprime les objets du compartiment"](#) option de suppression de tous les objets d'un compartiment.
- Le compartiment dispose d'une configuration en cycle de vie, qui expire.
- La dernière période de la règle ILM pour l'objet se termine et aucun autre placement n'est spécifié.

Lorsque StorageGRID supprime un objet en raison d'une opération de suppression d'objets dans un compartiment, d'expiration du cycle de vie du compartiment ou d'expiration du placement ILM, l'objet répliqué n'est jamais supprimé d'une autre grille d'une connexion de fédération de grid. Toutefois, les marqueurs de suppression ajoutés au compartiment source par les suppressions du client S3 peuvent éventuellement être répliqués dans le compartiment de destination.

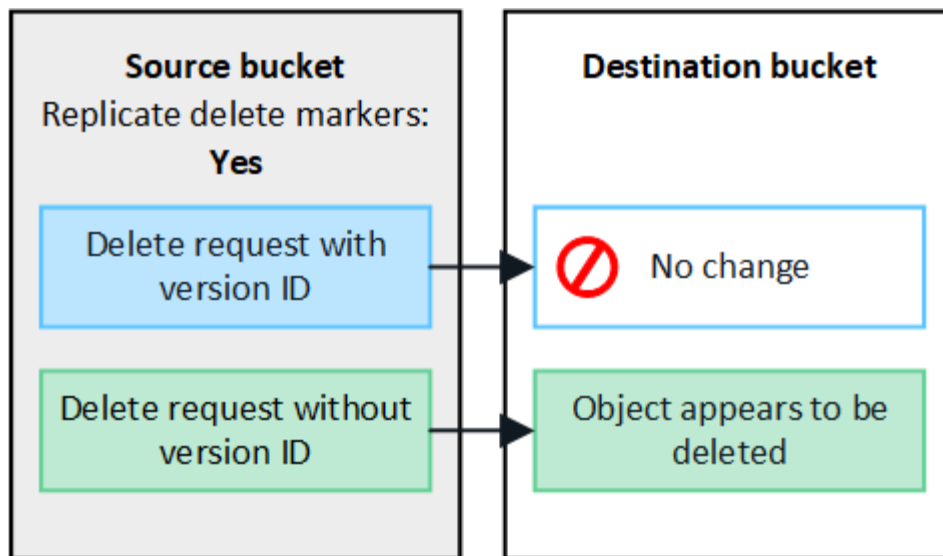
Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un compartiment dans lequel la réplication inter-grid est activée, vérifiez comment les clients S3 suppriment des objets des compartiments pour lesquels la gestion de version est activée, comme suit :

- Si un client S3 émet une demande de suppression qui inclut un ID de version, cette version de l'objet est définitivement supprimée. Aucun marqueur de suppression n'est ajouté au godet.
- Si un client S3 émet une demande de suppression qui n'inclut pas d'ID de version, StorageGRID ne supprime aucune version d'objet. Au lieu de cela, il ajoute un marqueur de suppression au bucket. Le marqueur de suppression oblige StorageGRID à agir comme si l'objet avait été supprimé :
 - Une requête GetObject sans ID de version échoue avec 404 No Object Found
 - Une demande GetObject avec un ID de version valide réussit et renvoie la version de l'objet demandée.

Lorsqu'un client S3 supprime un objet d'un compartiment pour lequel la réplication inter-grid est activée, StorageGRID détermine s'il faut répliquer la demande de suppression vers la destination, comme suit :

- Si la demande de suppression inclut un ID de version, cette version d'objet est définitivement supprimée de la grille source. Cependant, StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, de sorte que la même version d'objet n'est pas supprimée de la destination.
- Si la demande de suppression n'inclut pas d'ID de version, StorageGRID peut éventuellement répliquer le marqueur de suppression, en fonction de la configuration de la réplication inter-grille pour le bucket :
 - Si vous choisissez de répliquer les marqueurs de suppression (par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué vers le compartiment de destination. En effet, l'objet semble être supprimé sur les deux grilles.
 - Si vous choisissez de ne pas répliquer les marqueurs de suppression, un marqueur de suppression est ajouté au 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-grid a été activée"](#) . Les demandes de suppression pour le bucket source qui incluent un ID de version ne suppriment pas les objets du bucket de destination. Les demandes de suppression pour le bucket source qui n'incluent pas d'ID de version semblent supprimer des objets dans le bucket de destination.



Si vous souhaitez que les suppressions d'objets restent synchronisées entre les grilles, créez les compartiments correspondants ["Configurations de cycle de vie S3"](#) sur les deux grilles.

Mode de réplication des objets chiffrés

Lorsque vous répliquez les objets entre les grilles à l'aide de la réplication multigrille, vous pouvez chiffrer des objets individuels, utiliser le chiffrement de compartiment par défaut ou configurer le chiffrement au niveau de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement de compartiment ou de grille par défaut avant ou après l'activation de la réplication entre plusieurs grilles pour un compartiment.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID) lors de l'ajout des objets au compartiment source. Utilisez l'`x-amz-server-side-encryption` en-tête de la requête et spécifiez `AES256`. Voir ["Utilisez le cryptage côté serveur"](#).



L'utilisation de SSE-C (chiffrement côté serveur avec clés fournies par le client) n'est pas prise en charge pour la réplication inter-grille. L'opération d'ingestion échouera.

Pour utiliser le cryptage par défaut pour un compartiment, utilisez une requête `PutBucketEncryption` et définissez le `SSEAlgorithm` paramètre sur `AES256`. Le chiffrement au niveau du compartiment s'applique à tous les objets ingérés sans l'`x-amz-server-side-encryption` en-tête de la demande. Voir ["Opérations sur les compartiments"](#).

Pour utiliser le cryptage au niveau de la grille, définissez l'option **Stored object Encryption** sur **AES-256**. Le chiffrement au niveau du grid s'applique aux objets qui ne sont pas chiffrés au niveau du compartiment ou qui sont ingérés sans l'en-tête de la `x-amz-server-side-encryption` demande. Voir ["Configurez 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 n'est pas propagée à l'objet répliqué. Au lieu de cela, l'objet répliqué utilise 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 du mode de chiffrement des objets source, StorageGRID applique les règles suivantes :

1. Utilisez l'`x-amz-server-side-encryption` en-tête d'ingestion, le cas échéant.
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.

Pour déterminer comment chiffrer les objets répliqués, StorageGRID applique les règles suivantes dans l'ordre suivant :

1. Utilisez le même chiffrement que l'objet source, sauf si cet objet utilise le chiffrement AES-128.
2. Si l'objet source n'est pas chiffré ou 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 de 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.

Réplication inter-grille avec S3 Object Lock

Vous pouvez configurer la réplication inter-grille entre les buckets StorageGRID avec S3 Object Lock activé dans les circonstances suivantes.

Lorsque le verrouillage d'objet S3 sur le bucket source est...	Et le verrouillage de l'objet S3 sur le bucket de destination est...
Activé	Activé
Désactivées	Activé



Vous pouvez activer le verrouillage d'objets S3 sur des compartiments existants, ce qui pourrait entraîner une mauvaise configuration ultérieure.



Lorsque le verrouillage d'objets S3 est activé sur le compartiment source, assurez-vous qu'il l'est également sur le compartiment de destination. Si le verrouillage d'objets S3 est désactivé sur le compartiment de destination, une erreur se produit lors de la réplication. Consultez ["Alertes et erreurs de réplication intergrid"](#).

Lorsque le verrouillage d'objet S3 sur le bucket source est activé :

- Les objets sont verrouillés avec des paramètres de rétention à la destination dans cet ordre :
 - a. Les valeurs d'en-tête de rétention de l'objet source pour :


```
x-amz-object-lock-mode
```

```
x-amz-object-lock-retain-until-date
```
 - b. La rétention par défaut du bucket source, si elle est définie.
 - c. La rétention par défaut du bucket de destination, si elle est définie.

La rétention par défaut du bucket de destination ne remplace pas les paramètres de rétention répliqués à partir de l'objet source.

- Vous pouvez définir le statut de conservation légale pour l'objet de destination en utilisant `x-amz-object-lock-legal-hold` lors du téléchargement de l'objet.
- Une erreur se produit si le locataire ou le bucket de destination ne prend pas en charge les paramètres de verrouillage d'objet S3 de l'objet source. Consultez ["Alertes et erreurs de réplication inter-grille."](#)

Lorsque le verrouillage d'objet S3 sur le bucket source est désactivé :

- Vous pouvez configurer la rétention par défaut sur le bucket de destination pour appliquer les paramètres de rétention S3 Object Lock à l'objet de destination.
- L'objet de destination ne peut pas définir un statut de conservation légale.

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 compartiments pour lesquels la réplication inter-grid est activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, 501 Not Implemented est retourné. Le message est Put (Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.

PutObjectRetention et PutObjectLegalHold ne sont pas pris en charge

Les requêtes PutObjectRetention et PutObjectLegalHold ne sont pas entièrement prises en charge pour les objets dans les buckets pour lesquels la réplication inter-grille est activée.

Si un client S3 émet une demande PutObjectRetention ou PutObjectLegalHold, les paramètres de l'objet source sont modifiés, mais les modifications ne sont pas appliquées à la destination.

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 est 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 est également répliqué sur la grille de destination sous forme de deux segments de 1 Go, même si la taille de segment maximale de cette grille est de 50 Mo.

Comparer la réplication inter-grilles et la réplication CloudMirror dans StorageGRID

Lorsque vous commencez à utiliser la fédération de grille, examinez les similarités et les différences entre ["réplication entre plusieurs grilles"](#) et ["Service de réplication StorageGRID CloudMirror"](#).



Vous ne pouvez pas utiliser CloudMirror sur un bucket répliqué par réplication inter-grille, et vice versa.

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Quel est l'objectif principal ?	Un système StorageGRID agit comme un système de reprise après incident. Les objets d'un compartiment peuvent être répliqués entre les grilles dans une ou les deux directions.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). La réplication CloudMirror crée une copie indépendante d'un objet dans une infrastructure S3 indépendante. Cette copie indépendante n'est pas utilisée comme sauvegarde, mais est 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 synchronisés avec l'autre grid. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs, qui sont également synchronisés. 4. Créez les compartiments correspondants sur chaque grille et activez la réplication inter-grille dans une ou les deux directions.	1. Un utilisateur de locataire configure la réplication CloudMirror en définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. 2. Tout compartiment appartenant à ce compte de locataire peut être configuré de manière à pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	• Un administrateur du grid configure la connexion et les locataires. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les compartiments.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un compartiment S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération du grid.	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
La gestion des versions d'objets est-elle requise ?	Oui, la gestion des versions d'objet doit être activée dans les compartiments source et de destination.	Non, la réplication CloudMirror prend en charge toute combinaison de compartiments sans version et avec version sur la source et la destination.

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Pourquoi déplacer des objets vers la destination ?	Les objets sont automatiquement répliqués lorsque ceux-ci sont ajoutés à un compartiment sur lequel la réplication inter-grid est activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment qui a été configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grid crée des objets versionnés et réplique l'ID de version du compartiment source vers le compartiment de destination. Cela permet de maintenir l'ordre des versions sur les deux grilles.	La réplication CloudMirror ne nécessite pas de compartiments prenant en charge la gestion des versions. CloudMirror peut donc uniquement gérer les commandes d'une clé au sein d'un site. Il n'y a aucune garantie que la commande sera maintenue pour les demandes à un objet sur un site différent.
Que se passe-t-il si un objet ne peut pas être répliqué ?	L'objet est placé dans la file d'attente de réplication, en fonction des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de plate-forme "Recommandations relatives à l'utilisation des services de plate-forme" (voir).
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, les métadonnées de son système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non. Lorsqu'un objet est répliqué vers un compartiment externe, les métadonnées de son système sont mises à jour. Les métadonnées diffèrent d'un emplacement à l'autre, selon le moment de l'ingestion et le comportement de l'infrastructure S3 indépendante.
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire les objets en faisant une demande au compartiment sur les deux grilles.	Les applications peuvent récupérer ou lire les objets en faisant une requête vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression comprenant un ID de version ne sont jamais répliquées dans la grille de destination. • Les demandes de suppression qui n'incluent pas d'ID de version ajoutent un marqueur de suppression au compartiment source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grid est configurée pour une seule direction, les objets du compartiment de destination peuvent être supprimés sans affecter la source.	Les résultats varient en fonction de l'état de gestion des versions des compartiments source et destination (qui ne doivent pas nécessairement être identiques) : • Si les deux compartiments sont versionnés, une demande de suppression ajoute un marqueur de suppression aux deux emplacements. • Si seul le compartiment source est versionné, une demande de suppression ajoute un marqueur de suppression à la source, mais pas à la destination. • Si aucun compartiment n'est versionné, une demande de suppression supprime l'objet de la source mais pas de la destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.

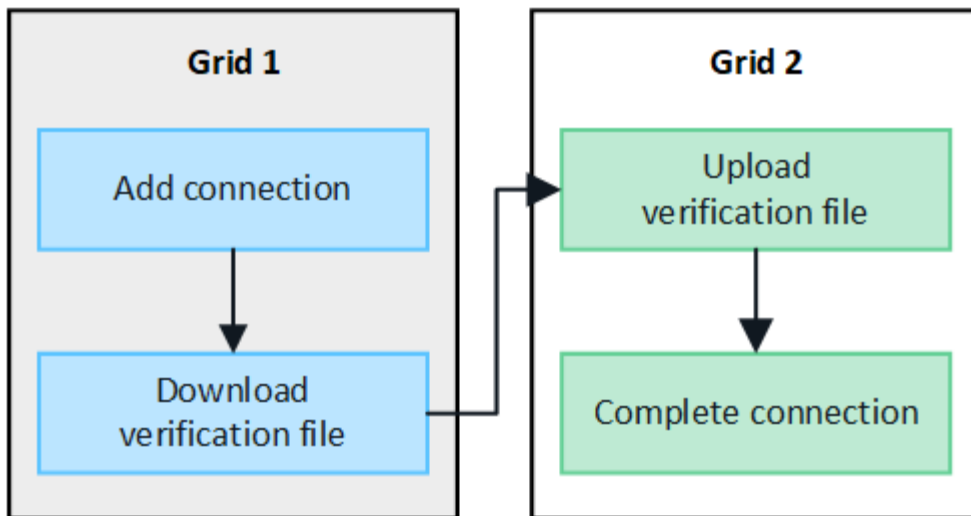
Créer des connexions de fédération de grille StorageGRID

Vous pouvez créer des connexions de fédération de grilles entre les systèmes StorageGRID si vous souhaitez synchroniser les détails des locataires et répliquer les données des objets.

Comme illustré dans la figure, la création d'une connexion de fédération de grille inclut des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la remplissez sur l'autre grille. Vous pouvez commencer à partir de n'importe quelle grille.



Vous pouvez, si vous le souhaitez, "[automatiser la création, la modification et la maintenance des connexions de fédération de grid](#)".



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 complets (FQDN) pour chaque grille au lieu d'adresses IP ou VIP, vous savez quels noms utiliser et vous avez confirmé que le serveur DNS de chaque grille contient les entrées appropriées.
- Vous utilisez un "[navigateur web pris en charge](#)".
- Vous disposez des droits d'accès racine et de la phrase de passe de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un des deux systèmes StorageGRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez **Ajouter une connexion**.
4. Saisissez un nom de connexion, c'est-à-dire un nom unique qui vous permettra de reconnaître facilement cette connexion. Par exemple, Grid 1-Grid 2.
5. Si vous souhaitez "[configurer un espace de noms global](#)", sélectionnez **Activer l'espace de noms global**.
6. Sélectionnez **Continuer**.
7. Saisissez les détails de la grille, comme suit :

Champ	Description
FQDN ou IP pour cette grille	L'une des options suivantes : • Nom de domaine complet de la grille dans laquelle vous êtes actuellement connecté • Adresse VIP d'un groupe haute disponibilité sur cette grille • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur cette grille. L'adresse IP peut se trouver sur n'importe quel réseau que la grille de destination peut atteindre.
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez entrer n'importe quel numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port. Vous devez vous assurer qu'aucun nœud d'une grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Nombre de jours pendant lesquels vous souhaitez que les certificats de sécurité pour cette grille dans la connexion soient valides. La valeur par défaut est 730 jours (2 ans), mais vous pouvez entrer une valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.
Phrase secrète de provisionnement pour cette grille	Phrase secrète de provisionnement de la grille à laquelle vous êtes connecté.
FQDN ou IP pour l'autre grille	L'une des options suivantes : • Nom de domaine complet de la grille à laquelle vous souhaitez vous connecter • Adresse VIP d'un groupe HA sur l'autre grid • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur l'autre grille. L'adresse IP peut se trouver sur n'importe quel réseau que la grille source peut atteindre.

1. Sélectionnez **Enregistrer et continuer**.

2. Pour l'étape Télécharger le fichier de vérification, sélectionnez **Télécharger le fichier de vérification**.

Une fois la connexion terminée sur l'autre grille, vous ne pouvez plus télécharger le fichier de vérification depuis l'une ou l'autre grille.

3. Localisez le fichier téléchargé (*connection-name.grid-federation*) et enregistrez-le dans un emplacement sûr.



Ce fichier contient des secrets (masqués en tant que ★) et d'autres détails sensibles et doit être stocké et transmis en toute sécurité.

4. Sélectionnez **Fermer** pour revenir à la page de fédération de grille.
5. Vérifiez que la nouvelle connexion est affichée et que son **état de connexion** est **en attente de connexion**.
6. Fournissez le `connection-name.grid-federation` fichier à l'administrateur de grille pour l'autre grille.

Connexion complète

Procédez comme suit sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page Télécharger.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, naviguez jusqu'au fichier téléchargé à partir de la première grille et sélectionnez `connection-name.grid-federation-le`.

Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours valides pour les certificats de sécurité de cette grille. Par défaut, l'entrée **Certificate valid Days** correspond à la valeur que vous avez entrée sur la première grille, mais chaque grille peut utiliser des dates d'expiration différentes.

En général, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.



Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner et les répliquions sont en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
7. Sélectionnez **Enregistrer et tester**.

Les certificats sont générés et la connexion est testée. Si la connexion est valide, un message de réussite s'affiche et la nouvelle connexion apparaît sur la page de fédération de grille. **État de la connexion** sera **connecté**.

Si un message d'erreur s'affiche, résoudre les problèmes éventuels. Voir "[Dépanner les erreurs de fédération de grille](#)".

8. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
9. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier d'origine ne peut pas être réutilisé.

Une fois que vous avez terminé

- Passez en revue les considérations relatives à "[gestion des locataires autorisés](#)".

- "[Créez un ou plusieurs nouveaux comptes de locataire](#)", Attribuez l'autorisation **utiliser la connexion de fédération de grille** et sélectionnez la nouvelle connexion.
- "[Gérer la connexion](#)" selon les besoins. Vous pouvez modifier les valeurs de connexion, tester une connexion, faire pivoter les certificats de connexion ou supprimer une connexion.
- "[Surveiller la connexion](#)" Dans le cadre de vos activités de surveillance StorageGRID normales.
- "[Dépanner la connexion](#)", y compris la résolution de toute alerte et erreur liée à la synchronisation des comptes et à la réplication inter-grilles.

Automatisez les connexions de fédération de grilles dans StorageGRID

Après avoir installé et configuré deux systèmes StorageGRID ou plus exécutant la version 12.1 ou ultérieure, vous pouvez automatiser la création, la modification et la maintenance des connexions de fédération de grilles à l'aide du `manage-grid-federation.py` script Python et d'un fichier de configuration JSON.

Avant de commencer

- Toutes les grilles exécutent StorageGRID 12.1 ou une version ultérieure.
- Si l'authentification unique (SSO) est activée sur une grille quelconque, vous l'avez désactivée.
- Vous disposez d'une machine Linux avec Python 3.6 ou une version ultérieure installée.
- Vous connaissez l'emplacement des fichiers suivants dans l'archive d'installation :

Nom du fichier	Description
<code>manage-grid-federation.py</code>	Script Python utilisé pour automatiser la gestion des connexions de fédération de grilles
<code>manage-grid-federation.sample.json</code>	Exemple de fichier de configuration à utiliser avec le script

- Vous avez créé un `manage-grid-federation.json` fichier de configuration. Pour créer ce fichier, vous pouvez modifier l'exemple de fichier de configuration `manage-grid-federation.sample.json`.



Stockez les mots de passe d'administration de la grille et les phrases de passe de provisionnement de votre `manage-grid-federation.json` fichier de configuration dans un emplacement sécurisé. Si les informations d'identification sont omises du fichier, le script vous les demandera de manière interactive. Vous devez également conserver une copie de sauvegarde du fichier de configuration modifié dans un emplacement sécurisé.

Champs du fichier de configuration

Le fichier de configuration JSON est un tableau d'objets. Chaque objet représente une grille et prend en charge les champs suivants :

Champ	Obligatoire	Description
<code>nom d'hôte</code>	Oui	Nom d'hôte ou adresse IP du nœud d'administration pour la grille
<code>nom_grille</code>	Oui	Nom d'affichage de la grille (12 caractères maximum)

Champ	Obligatoire	Description
nom d'utilisateur	Non	Nom d'utilisateur de l'administrateur de la grille (demandé de façon interactive si omis)
mot de passe	Non	Mot de passe administrateur de la grille (demandé interactivement si omis)
phrase secrète	Non	Phrase secrète de provisionnement (demandée de manière interactive si omise)
ca_bundle	Non	Chemin d'accès à un ensemble de certificats d'autorité de certification personnalisés pour la vérification SSL
région	Non	Région S3 par défaut souhaitée pour les connexions à l'espace de noms global
CNAME	Non	CNAME souhaité pour les connexions à l'espace de noms global
globalEndpoint	Non	Point de terminaison d'espace de noms global souhaité



Si vous configurez l'un des champs d'espace de noms global (`region`, `CNAME`, `globalEndpoint`), vous devez fournir les trois pour chaque grille. Assurez-vous que les régions et les CNAME sont uniques d'une grille à l'autre, et que la `globalEndpoint` valeur est identique pour toutes les grilles.

Description de la tâche

Vous pouvez utiliser le `manage-grid-federation.py` script Python et le `manage-grid-federation.json` fichier de configuration pour automatiser la gestion des connexions de fédération de grilles. Le script effectue les opérations suivantes :

- S'authentifie auprès de chaque grid à l'aide de l'API de gestion Grid Management
- Vérifie que toutes les grilles exécutent StorageGRID 12.1 ou une version ultérieure
- Vérifie que l'authentification unique est désactivée sur chaque grille
- Récupère les connexions de fédération de grille existantes et la configuration S3
- Met à jour les paramètres de la région S3, du CNAME et du point de terminaison d'espace de noms global lorsqu'ils sont configurés
- Crée de nouvelles connexions de fédération de grilles pour toutes les paires de grilles qui ne sont pas encore connectées
- Modifie les connexions existantes lorsque les noms d'affichage ou les paramètres d'espace de noms globaux ont changé
- Affiche un résumé de toutes les connexions et de leur état



Vous pouvez également gérer les connexions de fédération de grilles à l'aide de l'interface utilisateur de Grid Manager ou directement via l'API de gestion de grille.

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.

2. Accédez au répertoire contenant le script.

Par exemple :

```
cd StorageGRID-Webscale-version/platform
```

où **plateforme** est `debs`, `rpms` ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

Par exemple :

```
./manage-grid-federation.py -i manage-grid-federation.json
```

Vous pouvez utiliser les options de ligne de commande suivantes :

Option	Défaut	Description
<code>-i, --input-json-file</code>	<i>(requis)</i>	Chemin d'accès au fichier de configuration JSON contenant la liste des grilles
<code>-b, --base-port</code>	23001	Numéro de port de départ pour les nouvelles connexions de fédération de grille
<code>--no-verify-ssl</code>	Vérification SSL activée	Désactive la vérification des certificats SSL pour les connexions locales au grid

Modifier les connexions existantes

Si le script détecte que des modifications sont nécessaires pour les connexions existantes — par exemple, parce que les noms d'affichage de la grille ont changé ou que les paramètres d'espace de noms globaux doivent être mis à jour — il affichera un résumé des modifications proposées et demandera une confirmation avant de procéder.

Lorsque des mises à jour de configuration S3 (`region`, `CNAME`, ou `globalEndpoint`) sont nécessaires sur des grilles dont l'espace de noms global est activé, le script doit désactiver temporairement cet espace de noms pour appliquer les modifications. Dans ce cas, un message de confirmation signalera l'interruption temporaire du routage :

```
*** Global Namespace Disable Required ***
Global Namespace must be disabled to update region/CNAME/globalEndpoint
settings.
Routing requests will not work until Global Namespace is re-enabled.
Grids requiring S3 updates: grid1.example.com, grid2.example.com
Proceed with these edits and the temporary routing outage? [y/N]:
```



Pendant la mise à jour de la configuration S3, l'espace de noms global est temporairement désactivé, les requêtes de routage de l'espace de noms global ne fonctionneront donc pas. Planifiez cette opération lors d'une fenêtre de maintenance.

Une fois que vous avez terminé

Vos connexions de fédération de grilles sont établies et configurées lorsque le script affiche un résumé de confirmation similaire à ce qui suit :

```
===== Newly Established Connections =====
  • Grid-A and Grid-B – grid-a.example.com and grid-b.example.com on port
  23001

Total new connections: 1

===== All Grid-Federation Connections =====
  Name              Source              Target              Port
Status      Global Namespace
  -----
  -----
  Grid-A and Grid-B grid-a.example.com  grid-b.example.com  23001  new
enabled

Total connections listed: 1

===== Grid S3 Configuration Summary =====
grid-a.example.com:
  Default Region: us-east-1
  CNAME: s3-a.example.com
  Global namespace endpoint: gn.example.com
grid-b.example.com:
  Default Region: us-west-1
  CNAME: s3-b.example.com
  Global namespace endpoint: gn.example.com
```

État de sortie

Code	Description
0	Script exécuté avec succès
1	La validation a échoué ou un appel d’API de la grille a renvoyé une erreur (vérifiez la sortie du journal)



En cas d’échec de connexion, le script poursuit le traitement des paires restantes et consigne tous les échecs dans la section « Connexions échouées » du résultat. Examinez les messages d’erreur et résolvez tout problème avant de relancer le script.

Découvrez l’espace de noms global pour la fédération de grid.

Un espace de noms global permet aux locataires d’accéder aux compartiments sur plusieurs systèmes StorageGRID. Lorsque l’espace de noms global est activé sur les

connexions de fédération de grilles, les requêtes S3 CreateBucket et ListBuckets ciblant le point de terminaison de l'espace de noms global peuvent être envoyées au point de terminaison d'équilibrage de charge de n'importe quelle grille et sont automatiquement acheminées vers la grille appropriée en fonction de la région de signature dans la requête.

Qu'est-ce qu'un espace de noms global ?

Un espace de noms global permet aux locataires d'accéder aux compartiments sur plusieurs systèmes StorageGRID. Lorsque l'espace de noms global est activé sur les connexions de fédération de grilles, les requêtes S3 CreateBucket et ListBuckets ciblant le point de terminaison de l'espace de noms global peuvent être envoyées au point de terminaison d'équilibrage de charge de n'importe quelle grille et sont automatiquement acheminées vers la grille appropriée en fonction de la région de signature dans la requête.



Vous devez configurer un résolveur DNS pour effectuer le mappage DNS des URL de compartiment vers une grille spécifique. Au besoin, consultez votre administrateur réseau pour vous assurer que le résolveur DNS est correctement configuré. Reportez-vous à ["Configurer la résolution DNS"](#).

StorageGRID n'impose pas l'unicité des noms de compartiments entre les grilles de l'espace de noms global, ainsi des compartiments portant le même nom peuvent exister sur différentes grilles. La région de signature dans la requête est utilisée pour déterminer quelle grille possède le compartiment et doit recevoir la requête.

Par exemple, si le grid A utilise la région `us-east-1` et que le grid B utilise la région `us-west-1`, une requête CreateBucket envoyée à n'importe quel grid avec la région `us-west-1` est automatiquement acheminée vers le grid B.

Pour plus d'informations sur la fédération de grilles, consultez ["Qu'est-ce que la fédération de grille ?"](#).

Exemple d'espace de noms global

Grille 1

- Région par défaut : `region-1`
- CNAME par défaut : `s3.region-1.company.com`
- Point de terminaison global : `s3.company.com`

Grille 2

- Région par défaut : `region-2`
- CNAME par défaut : `s3.region-2.company.com`
- Point de terminaison global : `s3.company.com`

Grille 3

- Région par défaut : `region-3`
- CNAME par défaut : `s3.region-3.company.com`
- Point de terminaison global : `s3.company.com`

CreateBucket et ListBuckets opérations

Si vous créez un compartiment (`bucket123`) avec une région de signature `region-2` et ciblez le point de terminaison global `s3.company.com`, toute grille qui reçoit la requête créera le compartiment sur Grid 2.

Opérations spécifiques aux compartiments et opérations générales sur les objets

Une fois un compartiment créé sur une grille donnée, votre résolveur DNS résoudra l'URL du compartiment vers le CNAME du compartiment et de la grille.

Dans [exemple ci-dessus](#), le résolveur DNS doit résoudre `bucket123.s3.company.com` en `bucket123.s3.grid3.company.com` (CNAME du bucket et de la grille). Autrement dit, toutes les requêtes sont envoyées directement à cette grille sans routage supplémentaire.

Exemple

`PutObject to bucket123.s3.company.com` se résout à `bucket123.s3.grid3.company.com`

Comportement de S3 avec un espace de noms global

Une fois l'espace de noms global entièrement configuré, le comportement S3 suivant s'applique.

Application de la région

Toutes les requêtes S3 adressées au point de terminaison d'espace de noms global, à l'exception de ["CreateBucket"](#) et ["Listseaux"](#), nécessitent que la région de signature dans l'en-tête d'authentification V4 corresponde à la région par défaut de la grille.

- Si la région de signature ne correspond pas, la requête est refusée avec l'erreur suivante :

```
An error occurred (AuthorizationHeaderMalformed) when calling the
<operation> operation: The authorization header is malformed; the region
'<signing-region>' is wrong; expecting '<grid-default-region>'
```

- L'application des restrictions régionales s'applique à tous les compartiments de la grille, y compris ceux qui ont été créés avant l'activation de l'espace de noms global.
- L'application des restrictions régionales ne concerne que les requêtes d'authentification V4. Les requêtes anonymes et V2 ne sont pas soumises à l'application des restrictions régionales.

Routage de CreateBucket

CreateBucket requests envoyées au point de terminaison de l'espace de noms global (`s3.company.com`) peuvent être dirigées vers le point de terminaison d'équilibrage de charge de n'importe quelle grille. La requête est automatiquement acheminée vers la grille dont la région par défaut correspond à la région de signature de la requête.

Par exemple :

- La grille A a une région par défaut `us-east-1` et la grille B a une région par défaut `us-west-1`.
- Un client envoie une requête CreateBucket à `s3.company.com` avec la région de signature `us-west-1`.
- Le DNS round-robin dirige la requête vers Grid A.

- La grille A achemine la requête vers la grille B.
- Le compartiment est créé sur Grid B.

Considérations supplémentaires pour CreateBucket :

- L'LocationConstraint`élément peut être défini sur n'importe quelle région par défaut ou non par défaut de la grille. Cela affecte uniquement la politique ILM, pas la grille qui crée le compartiment (contrairement au comportement d'AWS avec `us-east-1).
- La région de signature dans la requête détermine quelle grille crée le compartiment (la région de signature doit correspondre à la région par défaut de la grille cible).
- Les requêtes V4 pré-signées sont prises en charge.
- Les requêtes anonymes et V2 ne sont pas prises en charge pour le routage global des espaces de noms.

Routage ListBuckets

ListBuckets les requêtes envoyées au point de terminaison de l'espace de noms global sont acheminées de la même manière que les requêtes CreateBucket, en utilisant la région de signature pour déterminer la grille appropriée.

Ni les réponses HEAD Bucket ni ListBuckets n'incluent la région par défaut de la grille. La région par défaut est déduite de la région de signature, qui doit correspondre à la région par défaut de la grille.

Gestion des comptes et des clés d'accès

Les comptes locataires et les clés d'accès S3 peuvent être synchronisés entre toutes les grilles à l'aide de ["synchronisation des comptes"](#) l'espace de noms global, mais ce dernier fonctionne également lorsque chaque grille possède son propre ensemble de clés d'accès. Si vous utilisez des clés d'accès distinctes, assurez-vous que le client S3 utilise la clé d'accès appropriée lors de l'envoi de requêtes à chaque grille.

Et ensuite ?

Vous êtes maintenant prêt à ["configurer l'espace de noms global"](#).

Configurer un espace de noms global pour la fédération de grilles

Configurez un espace de noms global pour permettre aux locataires d'accéder aux compartiments sur plusieurs systèmes StorageGRID.

Pour plus d'informations sur l'espace de noms global, reportez-vous à ["Découvrez l'espace de noms global pour la fédération de grid."](#)

Avant de commencer

- Vous êtes connecté au Grid Manager sur chaque grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#) pour chaque grille.
- Vous avez examiné le ["considérations et exigences"](#) pour les connexions de fédération de grille.

Exigences pour la configuration de l'espace de noms global

- Toutes les grilles de l'espace de noms global doivent avoir des connexions de fédération de grilles avec l'espace de noms global activé entre chaque paire de grilles.

- Le nombre maximal de grilles pouvant participer à un seul espace de noms global est de 11 (la grille locale et 10 grilles distantes).



La limite de 10 grilles est imposée par le nombre total maximal de connexions de fédération de grilles prises en charge par un déploiement StorageGRID. La limite totale de connexions s'applique à **toutes** les connexions de fédération de grilles du déploiement, y compris celles pour lesquelles l'espace de noms global n'est pas activé. Vous devez donc vous assurer que l'espace de noms global entièrement connecté et toutes les connexions de fédération de grilles supplémentaires ne dépassent pas cette limite globale.

- Les clients S3 doivent utiliser l'authentification par signature version 4 (SigV4). Les requêtes anonymes et celles utilisant la signature version 2 ne sont pas prises en charge pour les opérations de routage d'espace de noms global.
 - Les requêtes signées normales sont spécifiées comme décrit à ["Authentification des requêtes : utilisation de l'en-tête d'autorisation \(AWS Signature Version 4\)"](#).
 - Les demandes pré-signées sont spécifiées comme décrit à ["Authentification des requêtes : utilisation des paramètres de requête \(AWS Signature Version 4\)"](#).

Nombre de connexions requises

Dans un espace de noms global, chaque paire de grilles doit être connectée. Le nombre de connexions nécessaires dépend du nombre de grilles :

Nombre de grilles	Nombre de connexions requises
2	1
3	3
4	6
5	10
n	$n \times (n - 1) / 2$

Étape 1 : Définissez une région par défaut unique pour chaque grille

Chaque grille de l'espace de noms global doit avoir une région par défaut unique. La région par défaut identifie la grille qui possède un compartiment.

CreateBucket et ListBuckets les requêtes sont acheminées en fonction de cette région, et toutes les autres requêtes doivent correspondre à la région par défaut vers laquelle elles sont envoyées.

Pour plus d'informations, consultez ["Configurer les régions S3"](#).

Étapes

1. Sur chaque grille, ["définissez la région par défaut sur une valeur unique"](#). Par exemple, définissez la grille A sur `us-east-1` et la grille B sur `us-west-1`.



Vous pouvez toujours utiliser des régions non par défaut, définies à l'aide de l'élément `LocationConstraint` dans "[CreateBucket demandes](#)", à des fins de politique ILM. Les régions non par défaut ne sont pas validées pour leur unicité entre les grilles de l'espace de noms global.

2. Répétez l'opération pour chaque grille de l'espace de noms global. Chaque grille doit avoir une région par défaut différente.
3. Configurez des régions supplémentaires selon les besoins.

Étape 2 : configurez les paramètres d'espace de noms globaux S3

Sur chaque grille de l'espace de noms global, vous ajoutez deux noms de domaine de point de terminaison S3 :

- Un point de terminaison d'espace de noms global identique sur toutes les grilles
- Un CNAME unique pour la grille

Vous configurerez votre DNS externe de sorte que le point de terminaison de l'espace de noms global se résolve vers une ou plusieurs grilles, et que les points de terminaison CNAME uniques se résolvent vers la grille spécifique.



Vous devez [configurer la région par défaut](#) avant de configurer les paramètres de l'espace de noms global S3. Lorsque vous activez les paramètres de l'espace de noms global, les requêtes S3 échoueront si elles ne spécifient pas la région correcte. Toutes les requêtes S3 doivent être signées avec la région par défaut de la grille.

Étapes

1. Sur chaque grille, sélectionnez **Configuration > Réseau > Noms de domaine des S3 endpoint > Noms de domaine**.
2. Ajoutez un nom de domaine de point de terminaison d'espace de noms global identique sur toutes les grilles. Par exemple : `s3.example.com`.
3. Ajoutez un enregistrement CNAME unique pour la grille. Par exemple, `s3.company.com`.
4. Sélectionnez **Enregistrer**.
5. Sélectionnez **Paramètres d'espace de noms globaux**.
 - a. Sélectionnez le point de terminaison de l'espace de noms global.
 - b. Sélectionnez le nom de domaine CNAME unique de la grille.
6. Sélectionnez **Enregistrer**.
7. Assurez-vous que les certificats serveur utilisés par les clients incluent les nouveaux noms de domaine des endpoints S3.
 - Si les clients se connectent à un noeud final d'équilibreur de charge qui utilise son propre certificat, "[mettez à jour le certificat associé au noeud final](#)".
 - Si les clients se connectent à un terminal d'équilibrage de charge qui utilise le certificat d'API S3 global ou directement aux nœuds de stockage, "[Mettez à jour le certificat d'API S3 global](#)".
8. Répétez ces étapes sur chaque grille de l'espace de noms global.

Pour plus de détails, consultez "[Configuration des noms de domaine de terminaux S3](#)".

Étape 3 : Créez des connexions de fédération de grille avec l'espace de noms global activé

Une fois les noms de domaine des points de terminaison S3 et les régions par défaut configurés sur toutes les grilles, vous pouvez créer des connexions de fédération de grilles avec l'espace de noms global activé.

Description de la tâche

Lorsque vous créez une connexion de fédération de grille et activez l'espace de noms global, les champs point de terminaison de l'espace de noms global, CNAME et région par défaut sont automatiquement renseignés avec les valeurs que vous avez configurées lors des étapes précédentes. Le Grid Manager empêche l'activation de l'espace de noms global si ces champs ne sont pas correctement définis.



Une fois qu'une connexion de fédération de grilles avec un espace de noms global est créée, le point de terminaison de l'espace de noms global, le CNAME et la région par défaut des grilles de cette connexion ne peuvent pas être modifiés.

Étapes

1. Sur la première grille, suivez les étapes décrites dans ["Créer des connexions de fédération de grille"](#).
2. Lors de la saisie des informations de connexion, sélectionnez **Activer l'espace de noms global**.

Les champs relatifs au point de terminaison de l'espace de noms global, au CNAME et à la région par défaut sont automatiquement renseignés avec les valeurs que vous avez configurées lors des étapes précédentes. Si l'une de ces valeurs est manquante ou invalide, vous ne pourrez pas activer l'espace de noms global tant que vous n'aurez pas résolu ces problèmes.

3. Finalisez la connexion en téléchargeant le fichier de vérification et en le téléversant sur l'autre grille.
4. Répétez les étapes précédentes pour chaque paire de grilles dans l'espace de noms global.

Par exemple, avec 3 grilles, vous avez besoin de 3 connexions (Grille A–Grille B, Grille A–Grille C, Grille B–Grille C). Avec 4 grilles, vous avez besoin de 6 connexions. Vous pouvez avoir un maximum de 10 grilles dans un espace de noms global. Reportez-vous à [Nombre de connexions requises](#).

Étape 4 : Configurer les points de terminaison de l'équilibreur de charge

["Configurer un point de terminaison d'équilibrage de charge"](#) pour chaque grid dans le global namespace. Utilisez le même port pour chacun de ces endpoints.



Assurez-vous de configurer les points de terminaison de l'équilibreur de charge avant de configurer la résolution DNS.

Étape 5 : Configurer la résolution DNS

StorageGRID ne fournit pas de résolveur DNS intégré pour l'espace de noms global. Vous devez configurer votre infrastructure DNS externe pour acheminer les requêtes S3 vers la grille appropriée.

Votre résolveur DNS doit :

1. Résolvez le point de terminaison de l'espace de noms global (par exemple, `s3.example.com`) vers les points de terminaison de l'équilibreur de charge d'une ou plusieurs grilles, généralement en utilisant le DNS round-robin.
2. Résolvez le CNAME unique de chaque grille (par exemple, `s3.grid-a.example.com`) vers les points de terminaison de l'équilibreur de charge pour cette grille spécifique.

3. Pour les requêtes de compartiment de style hébergé virtuel (par exemple, `bucket.s3.example.com`), utilisez la politique de routage de votre organisation pour associer les noms de compartiment au CNAME de la grille appropriée.

StorageGRID ne propose pas de mécanisme basé sur DNS pour découvrir quelle grille possède un bucket. Si vous avez besoin d'un routage automatique basé sur la propriété du bucket, utilisez la "[API de gestion des locataires](#)" pour émettre des requêtes ListBucket afin d'obtenir les UUID des buckets. Maintenez une correspondance interne entre les UUID des buckets et les grilles. Votre DNS externe doit utiliser cette correspondance plutôt que d'interroger directement StorageGRID.

Informations associées

- "[Qu'est-ce que la fédération de grille ?](#)"
- "[Créer des connexions de fédération de grille](#)"
- "[Configuration des noms de domaine de terminaux S3](#)"
- "[Gérer les connexions de fédération de grille](#)"

Gérer les connexions de fédération de grille StorageGRID

La gestion des connexions de fédération de grille entre les systèmes StorageGRID inclut la modification des détails de connexion, la rotation des certificats, la suppression des autorisations de locataire et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Autorisation d'accès racine](#)" pour la grille à laquelle vous êtes connecté.

modifiez une connexion de fédération de grille

Vous pouvez modifier une connexion de fédération de grille en vous connectant au nœud d'administration principal sur l'une des grilles de la connexion. Après avoir apporté des modifications à la première grille, vous devez télécharger un nouveau fichier de vérification et le télécharger sur l'autre grille.



Pendant la modification de la connexion, les demandes de synchronisation de compte ou de réplication inter-grilles continueront d'utiliser les paramètres de connexion existants. Vous devez modifier une connexion à la fois et téléverser un fichier de vérification sur la grille distante pour chaque connexion. Les modifications sont appliquées après avoir été téléversées sur les grilles distantes.

Commencez à modifier la connexion

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **Nœuds** 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 de candidat sur tous les nœuds d'administration de la première grille. Si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, un message d'avertissement s'affiche lorsque vous sélectionnez **Enregistrer et tester**.

3. Sélectionnez **Configuration > Système > Fédération de grille**.
4. Modifiez les détails de la connexion à l'aide du menu **actions** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique. Reportez-vous à la section "[Créer des connexions de fédération de grille](#)" pour savoir ce que vous devez saisir.

Menu actions

- a. Sélectionnez le bouton radio de la connexion.
- b. Sélectionnez **actions > Modifier**.
- c. Entrez les nouvelles informations.

Page de détails

- a. Sélectionnez un nom de connexion pour afficher ses détails.
- b. Sélectionnez **Modifier**.
- c. Entrez les nouvelles informations.

5. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes connecté.
6. Sélectionnez **Enregistrer et continuer**.

Les nouvelles valeurs sont enregistrées, mais elles ne seront pas appliquées à la connexion tant que vous n'aurez pas téléchargé le nouveau fichier de vérification sur l'autre grille.

7. Sélectionnez **Télécharger le fichier de vérification**.

Pour télécharger ce fichier ultérieurement, rendez-vous sur la page de détails de la connexion.

8. Localisez le fichier téléchargé (*connection-name.grid-federation*) et enregistrez-le dans un emplacement sûr.



Le fichier de vérification contient des secrets et doit être stocké et transmis en toute sécurité.

9. Sélectionnez **Fermer** pour revenir à la page de fédération de grille.
10. Vérifiez que l'état de la **connexion** est **en attente de modification**.



Si l'état de la connexion était autre que **connecté** lorsque vous avez commencé à modifier la connexion, il ne passera pas à **modification en attente**.

11. Fournissez le *connection-name.grid-federation* fichier à l'administrateur de 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. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page de téléchargement.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé à partir de la première grille.
5. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
6. Sélectionnez **Enregistrer et tester**.

Si la connexion peut être établie à l'aide des valeurs modifiées, un message de réussite s'affiche. Sinon, un message d'erreur s'affiche. Passez en revue le message et répondez à tout problème.

7. Fermez l'assistant pour revenir à la page de fédération de grille.
8. Vérifiez que l'état de la **connexion** est **connecté**.
9. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
10. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

Tester une connexion de fédération de grille

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Testez la connexion à l'aide du menu **actions** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique.

Menu actions

- a. Sélectionnez le bouton radio de la connexion.
- b. Sélectionnez **actions > Test**.

Page de détails

- a. Sélectionnez un nom de connexion pour afficher ses détails.
- b. Sélectionnez **Tester la connexion**.

4. Vérifiez l'état de la connexion :

État de la connexion	Description
Connecté	Les deux grilles sont connectées et communiquent normalement.

État de la connexion	Description
Erreur	La connexion est en état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
Modification en attente	Vous avez modifié la connexion sur cette grille, mais la connexion utilise toujours la configuration existante. Pour terminer la modification, téléchargez le nouveau fichier de vérification sur l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais la connexion n'a pas été effectuée sur l'autre grille. Téléchargez le fichier de vérification à partir de cette grille et téléchargez-le sur l'autre grille.
Inconnu	La connexion est dans un état inconnu, probablement en raison d'un problème de mise en réseau ou d'un nœud hors ligne.

- Si l'état de la connexion est **Error**, résolvez les problèmes éventuels. Ensuite, sélectionnez de nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

faire pivoter les certificats de connexion

Chaque connexion de fédération de grille utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats.



Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner et les répliquions sont en attente jusqu'à ce que les certificats soient mis à jour.

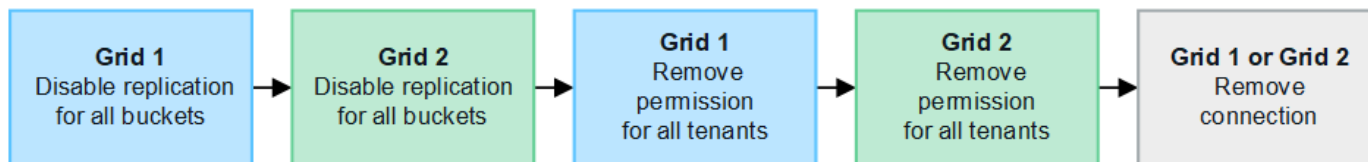
Étapes

- Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
- Sélectionnez **Configuration > Système > Fédération de grille**.
- Dans l'un des onglets de la page fédération de grille, sélectionnez le nom de la connexion pour afficher ses détails.
- Sélectionnez l'onglet **certificats**.
- Sélectionnez **faire pivoter les certificats**.
- Spécifiez le nombre de jours pendant lesquels les nouveaux certificats doivent être valides.
- Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes connecté.
- Sélectionnez **faire pivoter 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.

supprime une connexion de fédération de grille

Vous pouvez supprimer une connexion de fédération de grille de l'une des grilles de la connexion. Comme indiqué dans la figure, vous devez effectuer les étapes préalables sur les deux grilles pour confirmer que la connexion n'est pas utilisée par un locataire sur l'une ou l'autre des grilles.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime pas les éléments qui ont déjà été copiés entre les grilles. Par exemple, les utilisateurs de tenant, les groupes et les objets qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre de ces grilles lorsque l'autorisation du tenant est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, la réplication de tous les objets en attente de réplication (ingérés mais pas encore répliqués sur l'autre grille) échouera définitivement.

Désactivez la réplication pour tous les compartiments de locataires

Étapes

1. À partir de l'une des grilles, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **locataires autorisés**, déterminez si la connexion est utilisée par un locataire.
5. Si des locataires sont répertoriés, demandez à tous les locataires de "[désactiver la réplication entre les grilles](#)" pour tous leurs compartiments sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Chaque compte de locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour chaque locataire

Une fois la réplication multigrille désactivée pour tous les compartiments de tenant, supprimez l'autorisation **utiliser la fédération de grid** de tous les locataires sur les deux grilles.

Étapes

1. Sélectionnez **Configuration > Système > Fédération de grille**.
2. Sélectionnez le nom de la connexion pour afficher ses détails.
3. Pour chaque locataire de l'onglet **locataires autorisés**, supprimez l'autorisation **utiliser la connexion de fédération de grille** de chaque locataire. Voir "[Gérer les locataires autorisés](#)".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Déposer la connexion

Étapes

1. Lorsqu'aucun locataire de l'une ou l'autre grille n'utilise la connexion, sélectionnez **Supprimer**.
2. Vérifiez le message de confirmation et sélectionnez **Supprimer**.

- Si la connexion peut être supprimée, un message de réussite s'affiche. La connexion de fédération de grille est maintenant supprimée des deux grilles.
- Si la connexion ne peut pas être supprimée (par exemple, elle est toujours en cours d'utilisation ou si une erreur de connexion s'est produite), un message d'erreur s'affiche. Vous pouvez effectuer l'une des opérations suivantes :
 - Résolvez l'erreur (recommandé). Voir ["Dépanner les erreurs de fédération de grille"](#).
 - Déposer la connexion par la force. Voir la section suivante.

supprime une connexion de fédération de grille par force

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas l'état **Connected**.

La suppression forcée supprime uniquement la connexion de la grille locale. Pour supprimer complètement la connexion, effectuez les mêmes étapes sur les deux grilles.

Étapes

1. Dans la boîte de dialogue de confirmation, sélectionnez **forcer la suppression**.

Un message de réussite s'affiche. Cette connexion de fédération de grille ne peut plus être utilisée. Cependant, la réplication entre les compartiments de locataires peut toujours être activée et certaines copies d'objet peuvent avoir déjà été répliquées entre les grilles dans la connexion.

2. À partir de l'autre grille de la connexion, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
3. Sélectionnez **Configuration > Système > Fédération de grille**.
4. Sélectionnez le nom de la connexion pour afficher ses détails.
5. Sélectionnez **Supprimer** et **Oui**.
6. Sélectionnez **forcer la suppression** pour supprimer la connexion de cette grille.

Gérer les locataires autorisés pour la fédération de grilles StorageGRID

Vous pouvez autoriser les comptes locataires S3 à utiliser une ou plusieurs connexions de fédération de grilles entre plusieurs systèmes StorageGRID. Lorsque les locataires sont autorisés à utiliser une connexion, des étapes spécifiques sont nécessaires pour modifier les détails du locataire ou pour retirer définitivement l'autorisation d'utiliser la connexion.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#) pour la grille à laquelle vous êtes connecté.
- Vous avez ["créé une connexion de fédération de grille"](#) entre deux grilles.
- Vous avez examiné les flux de travail pour ["synchronisation des comptes"](#) et ["réplication entre plusieurs grilles"](#).
- Comme requis, vous avez déjà configuré l'authentification unique (SSO) ou la fédération d'identités pour les deux grilles de la connexion. Voir ["Découvrez la synchronisation des comptes pour la fédération de grilles"](#).

Créez un locataire autorisé

Si vous souhaitez autoriser un compte locataire nouveau ou existant à utiliser une connexion de fédération de grille pour la synchronisation des comptes et la réplication inter-grilles, suivez les instructions générales pour "[Créer un locataire S3](#)" ou "[modifier un compte de locataire](#)" et tenez compte des points suivants :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille dans la connexion. La grille dans laquelle un locataire est créé est la *grille source du locataire*.
- L'état de la connexion doit être **connecté**.
- Lorsque le locataire est créé ou modifié pour activer l'autorisation **utiliser la connexion de fédération de grille**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille dans laquelle le locataire est répliqué est la grille de destination du locataire_.
- Les locataires des deux grilles auront les mêmes ID de compte, nom, description, quota et autorisations à 20 chiffres. Vous pouvez également utiliser le champ **Description** pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 s'affiche également pour le locataire répliqué dans la grille 2 : « ce locataire a été créé sur la grille 1 ».
- Pour des raisons de sécurité, le mot de passe d'un utilisateur root local n'est pas copié dans la grille de destination.



Pour qu'un utilisateur root local puisse se connecter au tenant répliqué sur la grille de destination, un administrateur de grille pour cette grille doit "[modifier le mot de passe de l'utilisateur root local](#)".

- Une fois que le nouveau locataire ou le locataire modifié est disponible sur les deux grilles, les utilisateurs du tenant peuvent effectuer les opérations suivantes :
 - Depuis n'importe quelle grille connectée, créez des groupes et des utilisateurs locaux, qui sont automatiquement synchronisés avec toutes les autres grilles connectées. Voir "[Synchroniser les groupes de locataires et les utilisateurs](#)".
 - Créez de nouvelles clés d'accès S3 pour les utilisateurs locaux, qui sont automatiquement synchronisées avec les autres grilles connectées lorsque la synchronisation des clés d'accès est activée pour le locataire.



Les clés d'accès S3 des utilisateurs fédérés sont clonées une seule fois de la source vers la cible lors de leur création. Si ces clés d'accès S3 sont supprimées, ces modifications ne sont pas synchronisées avec les autres grilles. Vous devez supprimer manuellement les clés d'accès S3 sur les autres grilles.

- Créez des compartiments identiques sur les deux grilles dans la connexion et activez la réplication de type grille dans une direction ou dans les deux directions. Voir "[Gérer la réplication entre les grilles](#)".

Afficher un locataire autorisé

Vous pouvez afficher les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **Locataires**.
2. Sur la page tenants, sélectionnez le nom du locataire pour afficher la page des détails du locataire.
3. Vous pouvez également sélectionner l'onglet **Fédération de grilles** pour "[surveillez les connexions de la fédération du grid](#)".

Modifier un locataire autorisé

Si vous devez modifier un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales pour "[modification d'un compte de locataire](#)" et notez ce qui suit :

- Si un locataire possède l'autorisation **Utiliser la connexion de fédération de grille** :
- Vous pouvez modifier les informations du locataire depuis n'importe quelle grille de la connexion. Les modifications apportées aux paramètres au niveau du locataire (tels que le nom, la description ou le quota), ainsi qu'aux groupes, aux utilisateurs locaux et aux clés d'accès S3 détenues par les utilisateurs locaux, sont automatiquement synchronisées avec toutes les grilles connectées.
- Vous pouvez modifier les **connexions de fédération de grilles autorisées uniquement sur la grille source**.
- Vous pouvez ajouter une nouvelle connexion de fédération de grille.



Vous ne pouvez pas désélectionner les connexions existantes. Pour supprimer une connexion, accédez à la page de détails du locataire, sélectionnez l'onglet **Grid federation** et supprimez l'autorisation.

- Si vous ajoutez une nouvelle connexion lors de la modification d'un locataire, ce locataire sera répliqué sur la grille distante spécifiée par cette nouvelle connexion.

Supprimer un locataire autorisé



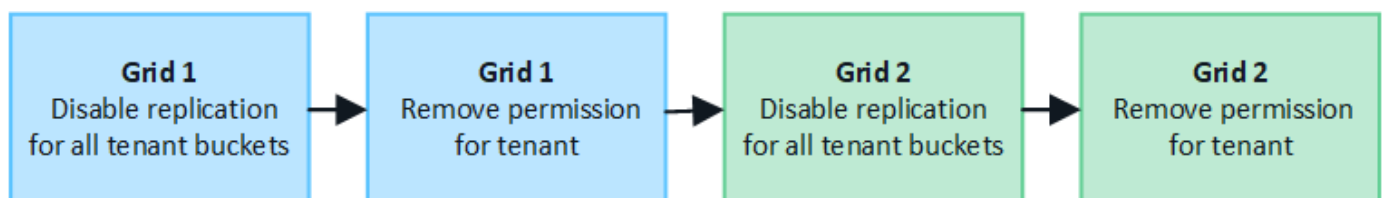
Si vous supprimez le locataire d'origine de la grille source ou le locataire synchronisé de la grille de destination, le locataire est supprimé de toutes les grilles, de sorte que le compte ne peut plus être utilisé.

Si vous devez supprimer un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales pour "[suppression d'un compte de locataire](#)" et notez ce qui suit :

- Avant de pouvoir supprimer le locataire sur la grille source, vous devez supprimer tous les compartiments pour le compte sur la grille source.
- Avant de pouvoir supprimer le locataire synchronisé sur la grille de destination, vous devez supprimer tous les compartiments du compte sur la grille de destination.
- Si vous supprimez le locataire d'origine ou le locataire synchronisé, le compte ne pourra plus être utilisé pour la réplication inter-grille.
- Si vous supprimez le locataire d'origine sur la grille source ou sur une grille de destination, les groupes de locataires, les utilisateurs et les clés synchronisés avec les grilles de destination sont également supprimés.

Supprimer l'autorisation de connexion utiliser la fédération de grille

Pour empêcher un locataire d'utiliser une connexion de fédération de grille, vous devez supprimer l'autorisation **utiliser la connexion de fédération de grille**.



Avant de supprimer l'autorisation d'un locataire d'utiliser une connexion de fédération de grille, notez ce qui suit :

- Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments du locataire. Le compte de locataire doit d'abord désactiver la réplication inter-grid pour tous ses compartiments.
- La suppression de l'autorisation **utiliser la connexion de fédération de grille** ne supprime pas les éléments qui ont déjà été répliqués entre les grilles. Par exemple, les utilisateurs, groupes et objets de tenant qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre des grilles lorsque l'autorisation du tenant est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- 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 de fédération de grille** fait de la grille locale la grille source et déclenche la synchronisation vers la grille distante spécifiée par la connexion de fédération de grille sélectionnée. Si le compte locataire existe déjà sur la grille distante, la synchronisation entraînera une erreur de conflit.

Avant de commencer

- Vous utilisez un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#) pour les deux grilles.

Désactivez la réplication pour les compartiments de locataires

Dans un premier temps, désactivez la réplication inter-grid pour tous les compartiments de locataires.

Étapes

1. À partir de l'une des grilles, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **locataires autorisés**, déterminez si le locataire utilise la connexion.
5. Si le locataire est répertorié, demandez-lui de vous indiquer ["désactiver la réplication entre les grilles"](#) tous ses compartiments sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Le locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour le locataire

Une fois la réplication multigrille désactivée pour les compartiments de tenant, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération GRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.

2. Supprimez l'autorisation de la page grid federation ou de la page tenants.

Page de fédération de grille

- a. Sélectionnez **Configuration > Système > Fédération de grille**.
- b. Sélectionnez le nom de la connexion pour afficher sa page de détails.
- c. Dans l'onglet **locataires autorisés**, sélectionnez le bouton radio du locataire.
- d. Sélectionnez **Supprimer l'autorisation**.

Page locataires

- a. Sélectionnez **Locataires**.
- b. Sélectionnez le nom du locataire pour afficher la page de détails.
- c. Dans l'onglet **grid federation**, sélectionnez le bouton radio de la connexion.
- d. Sélectionnez **Supprimer l'autorisation**.

3. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

- Si l'autorisation peut être supprimée, vous êtes renvoyé à la page des détails et un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.
- Si la réplication entre plusieurs compartiments de tenant est toujours activée, une erreur s'affiche.

 **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.) Connectez-vous au gestionnaire de locataires et désactivez la réplication pour chaque compartiments du locataire. Voir "[Gérer la réplication entre les grilles](#)". Répétez ensuite les étapes pour supprimer l'autorisation **utiliser la connexion grille**.
- Supprimez l'autorisation par force. Voir la section suivante.

4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation pour le même locataire sur l'autre grille.

supprimez l'autorisation par la force

Si nécessaire, vous pouvez forcer la suppression de l'autorisation d'un locataire à utiliser une connexion de fédération de grille, même si la réplication inter-grid est activée dans les compartiments de locataires.

Avant de supprimer l'autorisation d'un locataire par la force, notez les considérations générales [suppression de l'autorisation](#) et les considérations supplémentaires suivantes :

- Si vous supprimez l'autorisation **utiliser la connexion de fédération de grille** par force, tous les objets en attente de réplication vers l'autre grille (ingérés mais pas encore répliqués) continueront d'être répliqués. Pour empêcher ces objets en cours d'exécution d'atteindre le compartiment de destination, vous devez

également supprimer l'autorisation du locataire sur l'autre grille.

- Tous les objets ingérés dans le compartiment source après la suppression de l'autorisation **utiliser la connexion de fédération de grille** ne seront jamais répliqués dans le compartiment de destination.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **Configuration > Système > Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher sa page de détails.
4. Dans l'onglet **locataires autorisés**, sélectionnez le bouton radio du locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **forcer la suppression**.

Un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.

7. Si nécessaire, accédez à l'autre grille et répétez ces étapes pour forcer la suppression de l'autorisation pour le même compte de tenant sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours d'atteindre le compartiment de destination.

Dépanner les erreurs de fédération de grille dans StorageGRID

Vous pourriez avoir besoin de résoudre les alertes et les erreurs liées aux connexions de fédération de grilles, à la synchronisation des comptes et à la réplication inter-grilles.

alertes et erreurs de connexion de fédération de grille

Vous pouvez recevoir des alertes ou rencontrer des erreurs avec vos connexions de fédération de grille.

Après avoir effectué des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion revient à **connecté**. Pour obtenir des instructions, reportez-vous à la section "[Gérer les connexions de fédération de grille](#)".

Alerte d'échec de la connexion de fédération de grille

Problème

L'alerte **échec de la connexion de fédération de grille** a été déclenchée.

Détails

Cette alerte indique que la connexion de fédération de grille entre les grilles ne fonctionne pas.

Actions recommandées

1. Vérifiez les paramètres de la page de fédération de grille pour les deux grilles. Vérifier que toutes les valeurs sont correctes. Voir "[Gérer les connexions de fédération de grille](#)".
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a pas d'alertes pour les certificats de fédération de grille expirés et que les détails de chaque certificat sont valides. Reportez-vous aux instructions relatives à la rotation "[Gérer les connexions de fédération de grille](#)" des certificats de connexion dans .
3. Vérifiez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez les alertes susceptibles d'affecter ces nœuds et réessayez.

4. Si vous avez fourni un nom de domaine complet (FQDN) pour la grille locale ou distante, vérifiez que le serveur DNS est en ligne et disponible. Reportez-vous à la section ["Qu'est-ce que la fédération de grille ?"](#) pour connaître la configuration réseau, l'adresse IP et DNS requise.

Expiration de l'alerte de certificat de fédération de grille

Problème

L'alerte **expiration du certificat de fédération de grille** a été déclenchée.

Détails

Cette alerte indique qu'un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.

Actions recommandées

Reportez-vous aux instructions relatives à la rotation ["Gérer les connexions de fédération de grille"](#) des certificats de connexion dans .

Erreur lors de la modification d'une connexion de fédération de grille

Problème

Lors de la modification d'une connexion de fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : "Echec de la création d'un fichier de configuration de candidat sur un ou plusieurs nœuds."

Détails

Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de configuration de candidat sur tous les nœuds d'administration de la première grille. Un message d'avertissement s'affiche si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, par exemple, parce qu'un nœud d'administration est hors ligne.

Actions recommandées

1. Dans la grille que vous utilisez pour modifier la connexion, sélectionnez **Nœuds**.
2. Vérifiez que tous les nœuds d'administration de ce grid sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et réessayez de modifier la connexion.

Erreurs de synchronisation du compte

Impossible de se connecter à un compte locataire synchronisé

Problème

Impossible de vous connecter à un compte locataire synchronisé. Le message d'erreur sur la page de connexion du Tenant Manager est : « Vos identifiants pour ce compte étaient invalides. Veuillez réessayer. »

Détails

Le mot de passe que vous définissez pour l'utilisateur racine local du locataire et les autres utilisateurs locaux est automatiquement synchronisé. Toutefois, vous devrez peut-être modifier le mot de passe de l'utilisateur racine local du locataire sur la grille de destination avant de pouvoir vous connecter au compte du locataire sur cette grille.

Actions recommandées

Pour que l'utilisateur root puisse se connecter à la grille de destination du locataire, l'administrateur de la grille doit d'abord se connecter ["modifiez le mot de passe de l'utilisateur root local"](#) à la grille de destination.

Locataire créé sans synchronisation

Problème

Vous voyez le message « Tenant created without a sync » après avoir créé un nouveau locataire avec l'autorisation **Use grid federation connection**.

Détails

Ce problème peut se produire si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner la liste d'une connexion défectueuse sous le nom **connectée**.

Actions recommandées

1. Vérifiez la raison indiquée dans le message d'erreur et résolvez tout problème de réseau ou autre qui pourrait empêcher la connexion de fonctionner. Voir [Alertes et erreurs de connexion de fédération de grille](#).
2. Suivez les instructions pour tester une connexion de fédération de grille dans "[Gérer les connexions de fédération de grille](#)" pour vérifier 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 synchronisé.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer la synchronisation**. Si l'erreur a été résolue, le compte du locataire sera alors synchronisé avec l'autre grille.

Alertes et erreurs de réplication intergrid

Dernière erreur affichée pour la connexion ou le locataire

Problème

Quand "[affichage d'une connexion de fédération de grille](#)" (ou quand "[gestion des locataires autorisés](#)" pour une connexion), vous remarquez une erreur dans la colonne **dernière erreur** de la page des détails de la connexion. Par exemple :

Grid 1 - Grid 2

Local hostname (this grid):10.115.96.170

Port:23000

Remote hostname (other grid):10.115.96.175

Connection status:

Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Remove permissionClear errorSearch...

Displaying one result

Tenant name	Last error
Tenant A	2025-03-13 15:54:59 PDT 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. (logID 13371653720226059496) 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 sont 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 compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.
- L'objet source possède des paramètres de verrouillage d'objet S3 qui ne sont pas conformes aux paramètres de conservation au niveau du locataire de la grille de destination.
- L'objet source dispose de paramètres de verrouillage d'objet S3 et le verrouillage d'objet S3 est désactivé sur le bucket de destination.

Actions recommandées

Si un message d'erreur apparaît dans la colonne **dernière erreur**, procédez comme suit :

1. Vérifiez le texte du message.
2. Effectuez les actions recommandées.

Par exemple, si le versionnage a été suspendu sur le compartiment de destination pour la réplication inter-grilles, réactivez le versionnage pour ce compartiment. Ou, si S3 Object Lock a été désactivé sur le compartiment de destination pour la réplication inter-grilles, activez S3 Object Lock pour ce compartiment.

3. Sélectionnez le compte de connexion ou de locataire dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.



Après avoir dégagé l'erreur, une nouvelle **dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui présente également une erreur.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, reportez-vous à la section "[Identifier et réessayer les opérations de réplication ayant échoué](#)".

Alerte de défaillance permanente de la réplication multi-grid

Problème

L'alerte **échec permanent de la réplication Cross-grid** a été déclenchée.

Détails

Cette alerte indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux

grilles pour une raison qui nécessite une intervention de l'utilisateur. Cette alerte est généralement causée par une modification du compartiment source ou de destination.

Actions recommandées

1. Connectez-vous à la grille dans laquelle l'alerte a été déclenchée.
2. Accédez à **Configuration > Système > Fédération de grille** et recherchez le nom de connexion répertorié dans l'alerte.
3. Dans l'onglet locataires autorisés, consultez la colonne **dernière erreur** pour déterminer quels comptes de locataires ont des erreurs.
4. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "[Surveiller les connexions de fédération de grille](#)" pour consulter les mesures de réplication entre les grilles.
5. Pour chaque compte de locataire concerné :
 - a. Reportez-vous aux instructions de la "[Surveillez l'activité des locataires](#)" pour vérifier que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grid.
 - b. Si nécessaire, augmentez le quota du locataire sur la grille de destination pour permettre l'enregistrement de nouveaux objets.
6. Pour chaque locataire concerné, connectez-vous au Gestionnaire de locataires sur les deux grilles afin de comparer la liste des compartiments.
7. Pour chaque compartiment pour lequel la réplication inter-grid est activée, vérifiez les points suivants :
 - Il existe un compartiment correspondant pour le même locataire sur l'autre grille (doit utiliser le nom exact).
 - La gestion des versions des objets est activée dans les deux compartiments (la gestion des versions ne peut pas être suspendue sur les deux grilles).
 - Aucun compartiment n'est à l'état **Suppression d'objets : lecture seule**.
8. Pour vérifier que le problème a été résolu, reportez-vous aux instructions de la section "[Surveiller les connexions de fédération de grille](#)" pour vérifier les mesures de réplication inter-grille ou effectuez les opérations suivantes :
 - a. Retournez à la page Grid federation.
 - b. Sélectionnez le locataire affecté et sélectionnez **Effacer erreur** dans la colonne **dernière erreur**.
 - c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
 - d. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.



Une fois l'alerte résolue, il peut s'écouler jusqu'à un jour avant que l'alerte ne s'efface.

- a. Accédez à "[Identifier et réessayer les opérations de réplication ayant échoué](#)" pour identifier les objets ou supprimer les marqueurs qui n'ont pas pu être répliqués sur l'autre grille et pour réessayer la réplication si nécessaire.

Alerte de ressource de réplication inter-grid indisponible

Problème

L'alerte **ressource de réplication multigrille indisponible** a été déclenchée.

Détails

Cette alerte indique que les demandes de réplication inter-grid sont en attente car une ressource n'est pas disponible. Par exemple, une erreur réseau peut se produire.

Actions recommandées

1. Surveillez l'alerte pour voir si le problème se résout de lui-même.
2. Si le problème persiste, déterminez si l'une des grilles a une alerte **échec de la connexion de fédération de grille** pour la même connexion ou une alerte **impossible de communiquer avec le nœud** pour un nœud. Cette alerte peut être résolue lorsque vous résolvez ces alertes.
3. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "[Surveiller les connexions de fédération de grille](#)" pour consulter les mesures de réplication entre les grilles.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grid se poursuivra normalement une fois le problème résolu.

Identifier et réessayer les opérations de réplication StorageGRID ayant échoué

Après avoir résolu l'alerte **échec permanent de la réplication Cross-grid**, vous devez déterminer si des objets ou des marqueurs de suppression n'ont pas pu être répliqués sur l'autre grille. Vous pouvez ensuite réingérer ces objets ou utiliser l'API de gestion de grille pour réessayer la réplication.

L'alerte **échec permanent de la réplication multigrille** indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison qui nécessite une intervention de l'utilisateur pour la résoudre. Cette alerte est généralement causée par une modification du compartiment source ou de destination. Pour plus de détails, voir "[Dépanner les erreurs de fédération de grille](#)".

Déterminez si des objets n'ont pas pu être répliqués

Pour déterminer si des objets ou des marqueurs de suppression n'ont pas été répliqués sur l'autre grille, vous pouvez rechercher des messages dans le journal d'audit "[CGRR \(demande de réplication multigrille\)](#)". Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet en plusieurs parties ou un marqueur de suppression vers le compartiment de destination.

Vous pouvez utiliser pour traduire les "[outil d'audit-explication](#)" résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Recherchez les messages du CGRR sur le site `audit.log` et utilisez l'outil `audit-explication` pour formater les résultats.

Par exemple, cette commande gronde tous les messages CGRR au cours des 30 dernières minutes et utilise l'outil `audit-Explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {  
print }' audit.log | grep CGRR | audit-explain
```

Les résultats de la commande ressemblent à cet exemple, qui contient des entrées pour six messages CGRR. Dans l'exemple, toutes les demandes de réplication inter-grid ont renvoyé une erreur générale car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent les opérations « Replicate object » et les trois dernières sont pour les opérations « Replicate delete marker ».

```
CGRR Cross-Grid Replication Request tenant: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 croisée CGRR	Nom de la demande
locataire	ID de compte du locataire

Champ	Description
connexion	ID de la connexion de fédération de grille
fonctionnement	Type d'opération de réplication en cours de tentative : • répliquer l'objet • répliquer le marqueur de suppression • répliquer un objet multi pièce
godet	Nom du compartiment
objet	Nom de l'objet
version	ID de version de l'objet
erreur	Type d'erreur. Si la réplication de la grille croisée a échoué, l'erreur est « erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste d'objets et supprimé des marqueurs qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de l'une des deux manières suivantes :

- Réintégrez chaque objet dans le compartiment source.
- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
2. Sélectionnez **aller à la documentation privée de l'API**.



Les terminaux de l'API StorageGRID marqués « privé » sont susceptibles d'être modifiés sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

3. Dans la section **cross-grid-Replication-Advanced**, sélectionnez le noeud final suivant :

```
POST /private/cross-grid-replication-retry-failed
```

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez l'exemple de **versionID** par un ID de version du fichier audit.log correspondant à une demande de réplication croisée ayant échoué.

Veillez à conserver les guillemets doubles autour de la chaîne.

6. Sélectionnez **Exécuter**.
7. Vérifiez que le code de réponse du serveur est **204**, indiquant que l'objet ou le marqueur de suppression a

été marqué comme en attente pour la réplication de la grille transversale vers l'autre grille.



En attente signifie que la demande de réplication inter-grille a été ajoutée à la file d'attente interne pour traitement.

Surveiller les nouvelles tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles sont terminées.



La réplication d'un objet ou d'un marqueur de suppression vers une autre grille peut prendre plusieurs heures, voire plus.

Vous pouvez surveiller les nouvelles tentatives de deux manières :

- Utilisation d'un S3 ou d'"GetObject"une "Objet principal" demande. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• TERMINÉ : la réplication a réussi. • EN ATTENTE : l'objet n'a pas encore été répliqué. • ÉCHEC : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : l'objet a été répliqué à partir de la grille source.

- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. Dans la section **cross-grid-Replication-Advanced** de la documentation de l'API privée, sélectionnez le noeud final suivant :

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Sélectionnez **essayez-le**.
3. Dans la section paramètre, entrez l'ID de version que vous avez utilisé dans la `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Vérifiez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de la réplication, qui sera l'un des suivants :
 - **EN ATTENTE** : l'objet n'a pas encore été répliqué.
 - **TERMINÉ** : la réplication a réussi.
 - **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité dans StorageGRID

Vous pouvez configurer différents paramètres de sécurité à partir du Gestionnaire de grille pour sécuriser votre système StorageGRID.

Gestion du chiffrement

StorageGRID propose plusieurs options pour le chiffrement des données. Vous devez "[consultez les méthodes de cryptage disponibles](#)" déterminer lesquelles répondent à vos exigences en matière de protection des données.

Gérer les certificats

Vous pouvez "[configurer et gérer les certificats de serveur](#)" l'utiliser pour les connexions HTTP ou les certificats client utilisés pour authentifier l'identité d'un client ou d'un utilisateur sur le serveur.

Configurer les serveurs de gestion des clés

L'utilisation d'un "[serveur de gestion des clés](#)" vous permet de protéger vos données StorageGRID même si une appliance est retirée du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.



Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Node Encryption** pour chaque appliance au cours de l'installation, avant d'ajouter l'appliance à la grille.

Gérer les paramètres proxy

Si vous utilisez les services de plateforme S3 ou des pools de stockage cloud, vous pouvez configurer un "[serveur proxy de stockage](#)" entre les nœuds de stockage et les terminaux S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un "[serveur proxy d'administration](#)" entre les nœuds d'administration et le support technique.

Contrôle des pare-feu

Pour améliorer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques sur le "[pare-feu externe](#)". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "[pare-feu interne](#)". Vous pouvez empêcher l'accès à tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Étudiez les méthodes de cryptage StorageGRID

StorageGRID propose plusieurs options pour le chiffrement des données. Consultez les méthodes disponibles pour identifier les méthodes qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un récapitulatif détaillé des méthodes de cryptage disponibles dans StorageGRID.

Option de chiffrement	Comment cela fonctionne	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous " configurer un serveur de gestion des clés " pour le site StorageGRID et " activez le chiffrement des nœuds pour l'appliance ". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et déchiffre la clé de chiffrement des données (DEK) sur chaque volume.	Nœuds d'appliance sur lesquels Node Encryption est activé pendant l'installation. Toutes les données de l'appliance sont protégées contre les pertes ou les suppressions physiques du data Center. Remarque : la gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.
Page chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appliance contient des disques qui prennent en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase de passe pour un disque, il est impossible à quiconque de récupérer des données valides sur les disques qui ont été supprimés du système, sauf s'il connaît la phrase de passe. Avant de commencer l'installation, accédez à Configure Hardware > Drive Encryption pour définir une phrase de passe de lecteur qui s'applique à tous les disques à chiffrement automatique gérés par StorageGRID d'un nœud.	Les appliances contiennent des disques à chiffrement automatique. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Le chiffrement de disque ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'une appliance de stockage avec disques à chiffrement automatique et contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonction de sécurité des lecteurs est activée pour votre appliance StorageGRID, vous pouvez utiliser " SANtricity System Manager " pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Dispositifs de stockage équipés de disques Full Disk Encryption (FDE) ou de disques à autocryptage. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Utilisation avec certaines appliances de stockage ou avec des appliances de services impossible.

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement des objets stockés	Vous activez l'" Chiffrement des objets stockés " option dans le Gestionnaire de grille. Lorsqu'il est activé, tout nouvel objet non chiffré au niveau du compartiment ou de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées.
Chiffrement de compartiment S3	Vous lancez une demande PutBucketEncryption pour activer le cryptage du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur d'objets S3 (SSE)	Vous exécutez une demande S3 pour stocker un objet et inclure l'en- `x-amz-server-side-encryption` tête de la demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le cryptage côté serveur"
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande S3 pour stocker un objet et incluez trois en-têtes de requête. • x-amz-server-side-encryption-customer-algorithm • x-amz-server-side-encryption-customer-key • x-amz-server-side-encryption-customer-key-MD5	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. "Utilisez le cryptage côté serveur"

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. "Amazon simple Storage Service - Guide de l'utilisateur : protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement à la fois. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et utiliser la fonctionnalité de sécurité des disques de SANtricity System Manager pour « double chiffrement » des données sur les disques à chiffrement automatique des mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données des nœuds de l'appliance et utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lors de leur ingestion.

Si seule une petite partie de vos objets doit être cryptée, pensez à contrôler le chiffrement au niveau du compartiment ou de l'objet au niveau individuel. L'activation de plusieurs niveaux de chiffrement a un coût supplémentaire en termes de performance.

Informations associées

["En savoir plus sur les options de cryptage certifiées FIPS"](#)

Gérer les certificats

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur permettent d'établir des connexions sécurisées entre les clients et les serveurs, d'authentifier l'identité d'un serveur pour ses clients et de fournir un chemin de communication sécurisé pour les données. Le serveur et le client ont chacun une copie du certificat.
- **Certificats client** authentifient une identité client ou utilisateur au serveur, fournissant une authentification plus sécurisée que les mots de passe seuls. Les certificats client ne chiffrent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client compare 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 (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

StorageGRID dispose d'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.

Utilisez le certificat Grid CA pour les environnements hors production. Pour la production, utilisez des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont prises en charge mais non recommandées.

- Les certificats d'autorité de certification personnalisée ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent répondre au ["instructions de renforcement du système pour les certificats de serveur"](#).
- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé bundle de certificats d'autorité de certification).



StorageGRID inclut également des certificats CA du système d'exploitation identiques sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat d'autorité de certification du système d'exploitation.

Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations relatives à tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Depuis Grid Manager, 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 de navigateurs Web et de clients API externes.
- **Grid CA** : sécurise le trafic StorageGRID interne.
- **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
- **Noeuds finaux 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'identités ou des terminaux de service de plate-forme aux ressources de stockage S3.
- **Autre** : sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

Chaque onglet est décrit ci-dessous avec des liens vers des détails de certificat supplémentaires.

Mondial

Les certificats globaux sécurisent l'accès StorageGRID à partir de navigateurs Web et de clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- [Certificat de l'interface de gestion](#): Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID.
- [Certificat d'API S3](#): Sécurise les connexions API client aux nœuds de stockage, nœuds d'administration et nœuds de passerelle, que les applications client S3 utilisent pour télécharger et télécharger les données d'objet.

Les informations sur les certificats globaux installés comprennent :

- **Nom** : nom du certificat avec lien vers la gestion du certificat.
- **Description**
- **Type** : personnalisé ou par défaut. + vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité de la grille.
- **Date d'expiration** : si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
 - ["Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID"](#) Utilisé pour les connexions Grid Manager et tenant Manager.
 - ["Remplacez le certificat de l'API S3"](#) Utilisé pour les connexions de nœuds de stockage et de terminaux d'équilibrage de la charge (en option).
- ["Restaurez le certificat de l'interface de gestion par défaut"](#).
- ["Restaurez le certificat d'API S3 par défaut"](#).
- ["Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé"](#).
- Copiez ou téléchargez le ou le ["certificat de l'interface de gestion"](#) ["Certificat d'API S3"](#).

CA grille

Le [Certificat CA de la grille](#), généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic StorageGRID interne.

Les informations sur le certificat comprennent la date d'expiration du certificat et son contenu.

Vous pouvez ["Copiez ou téléchargez le certificat d'autorité de certification Grid"](#), mais vous ne pouvez pas le modifier.

Client

[Certificats client](#), Générée par une autorité de certification externe, sécurise les connexions entre les outils de contrôle externes et la base de données StorageGRID Prometheus.

La table de certificats possède une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que la date d'expiration du certificat.

Vous pouvez :

- ["Téléchargez ou générez un nouveau certificat client."](#)
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
 - ["Modifiez le nom du certificat client."](#)
 - ["Définissez l'autorisation d'accès Prometheus."](#)
 - ["Téléchargez et remplacez le certificat client."](#)
 - ["Copiez ou téléchargez le certificat client."](#)
 - ["Supprimez le certificat client."](#)
- Sélectionnez **actions** pour rapidement ["modifier"](#), ["attacher"](#) ou ["déposer"](#) un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions > Supprimer**.

Terminaux d'équilibrage de charge

[Certificats de noeud final de l'équilibreur de charge](#) Sécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

Le tableau des terminaux d'équilibrage de la charge comporte une ligne pour chaque terminal d'équilibrage de la charge configuré et indique si le certificat d'API S3 global ou le certificat de terminal d'équilibreur de charge personnalisé est utilisé pour le terminal. La date d'expiration de chaque certificat s'affiche également.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Vous pouvez :

- ["Afficher un point d'extrémité d'équilibreur de charge"](#), y compris les détails de son certificat.
- ["Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool."](#)
- ["Utilisez le certificat d'API S3 global"](#) au lieu de générer un nouveau certificat de point de terminaison d'équilibreur de charge.

Locataires

Les locataires peuvent utiliser [certificats de serveur de fédération des identités](#) ou [certificats de terminal du service de plate-forme](#) pour sécuriser leurs connexions avec StorageGRID.

La table de tenant dispose d'une ligne pour chaque locataire et indique si chaque locataire a l'autorisation d'utiliser ses propres services de référentiel d'identité ou de plate-forme.

Vous pouvez :

- ["Sélectionnez un nom de locataire pour vous connecter au Gestionnaire de tenant"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails de la fédération des identités du locataire"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails des services de plateforme du locataire"](#)
- ["Spécifiez un certificat de noeud final du service de plate-forme pendant la création du noeud final"](#)

Autre

StorageGRID utilise d'autres certificats de sécurité pour des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. Voici d'autres certificats de sécurité :

- [Certificats de pool de stockage cloud](#)
- [Certificats de notification d'alerte par e-mail](#)
- [Certificats de serveur syslog externe](#)
- [Certificats de connexion de fédération de grille](#)
- [Certificats de fédération des identités](#)
- [Certificats de serveur de gestion des clés \(KMS\)](#)
- [Certificats d'authentification unique](#)

Informations indique le type de certificat utilisé par une fonction et ses dates d'expiration de certificat de serveur et de client, le cas échéant. La sélection d'un nom de fonction ouvre un onglet de navigateur dans lequel vous pouvez afficher et modifier les détails du certificat.



Vous ne pouvez afficher et accéder aux informations relatives aux autres certificats que si vous disposez du ["autorisation appropriée"](#).

Vous pouvez :

- ["Spécification d'un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"](#)
- ["Spécifiez un certificat pour les notifications par e-mail d'alerte"](#)
- ["Utilisez un certificat pour un serveur syslog externe"](#)
- ["Faire pivoter les certificats de connexion de fédération de grille"](#)
- ["Afficher et modifier un certificat de fédération d'identités"](#)
- ["Télécharger les certificats du serveur de gestion des clés \(KMS\) et du client"](#)
- ["Spécifiez manuellement un certificat SSO pour une confiance de partie utilisatrice"](#)

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions d'implémentation.

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	Configuration > Sécurité > Certificats , sélectionnez l'onglet Global , puis sélectionnez Certificat d'interface de gestion	"Configurer les certificats d'interface de gestion"

Certificat d'API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées vers un nœud de stockage et les terminaux d'équilibrage de la charge (facultatif).	Configuration > Sécurité > Certificats , sélectionnez l'onglet Global , puis sélectionnez Certificat API S3	"Configurer les certificats d'API S3"

Certificat CA de la grille

Voir la [Description du certificat CA de la grille par défaut](#).

Certificat du client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes.	Configuration > Sécurité > Certificats puis sélectionnez l'onglet Client	"Configurer les certificats client"

Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un nœud final d'équilibreur de charge. Les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du certificat global Certificat d'API S3 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 nœud final de l'équilibreur de charge. Remarque : le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de l'StorageGRID.	Configuration > Réseau > Points de terminaison de l'équilibreur de charge	• "Configurer les terminaux de l'équilibreur de charge" • "Créez un nœud final d'équilibrage de charge pour FabricPool"

Certificat de terminal Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un StorageGRID Cloud Storage Pool à un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob Storage. Un certificat différent est requis pour chaque type de fournisseur de cloud.	ILM > pools de stockage	"Création d'un pool de stockage cloud"

Certificat de notification d'alerte par e-mail

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	Alertes > Configuration de la messagerie électronique	"Configurez les notifications par e-mail pour les alertes"

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui consigne les événements dans StorageGRID. Remarque : un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	Configuration > Surveillance > Serveur d'audit et syslog	"Utiliser un serveur syslog externe"

certificat de connexion de fédération de grille

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifier et crypter les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	Configuration > Système > Fédération de grille	• "Créer des connexions de fédération de grille" • "Faire pivoter les certificats de connexion"

Certificat de fédération des identités

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération des identités, ce qui permet de gérer les groupes et les utilisateurs d'administration par un système externe.	Configuration > Contrôle d'accès > Fédération d'identité	"Utiliser la fédération des identités"

Certificat de serveur de gestion des clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	Configuration > Sécurité > Serveur de gestion des clés	"Ajout d'un serveur de gestion des clés (KMS)"

Certificat de terminal des services de plate-forme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	Tenant Manager > STORAGE (S3) > Platform services Endpoints	"Créer un terminal de services de plate-forme" "Modifier le point final des services de plate-forme"

Certificat SSO (Single Sign-on)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identités, tels que Active Directory Federation Services (AD FS) et StorageGRID utilisés pour les demandes SSO (Single Sign-on).	Configuration > Contrôle d'accès > Authentification unique	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un nœud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 avec le terminal de l'équilibreur de charge et téléchargez le même certificat vers 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 une signature basée

sur la clé privée.

5. Le client compare 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 externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Types de certificats serveur pris en charge dans StorageGRID

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (algorithme de signature numérique de courbe elliptique).



Le type de chiffrement de la stratégie de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA requièrent des certificats ECDSA. Voir "[Gérer les certificats de sécurité](#)". Si vous configurez une stratégie de sécurité personnalisée qui n'est pas compatible avec le certificat de serveur, vous pouvez "[rétablir temporairement la stratégie de sécurité par défaut](#)".

Pour plus d'informations sur la façon dont StorageGRID sécurise les connexions client, reportez-vous à la section "[Sécurité pour les clients S3](#)".

Configurez les certificats d'interface de gestion dans StorageGRID

Vous pouvez remplacer le certificat de l'interface de gestion par défaut par un certificat personnalisé unique qui permet aux utilisateurs d'accéder à Grid Manager et au Gestionnaire de locataires sans rencontrer d'avertissement de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

Description de la tâche

Par défaut, chaque nœud d'administration est doté d'un certificat signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commun et une clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au tenant Manager. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, en fonction de l'autorité de certification racine (AC) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification Grid dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Gestionnaire de locataires.



Pour garantir que les opérations ne sont pas 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 à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous [restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée](#).

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (. key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : storagegrid_certificate.pem

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

Générez un certificat

Générez les fichiers de certificat du serveur.



La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisée signé par une autorité de certification externe.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.



Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page de certificat de l'interface de gestion affiche des informations détaillées sur le certificat pour les certificats en cours d'utilisation. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat de l'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid

Manager et tenant Manager.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client suivantes.

4. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` fichier.

Description de la tâche

La meilleure pratique pour un environnement de production consiste à utiliser un certificat signé par une autorité de certification externe.

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Pour `--domains`, utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple, `*.ui.storagegrid.example.com` utilise le caractère générique `*` pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com`.
- Définissez `--type` sur `management` pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.
- Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser l'argument `--days` 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 peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 720
```

Le résultat contient le certificat public requis par votre client de l'API de gestion.

4. Sélectionnez et copiez le certificat.

Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`

6. Vérifiez que le certificat a été configuré :

- a. Accédez au Grid Manager.
- b. Sélectionnez **Configuration > Sécurité > Certificats**
- c. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.

7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat de l'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le fichier de certificat ou de bundle CA .pem. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Configurer les certificats d'API S3 dans StorageGRID

Vous pouvez remplacer ou restaurer le certificat du serveur utilisé pour les connexions client S3 avec les nœuds de stockage ou pour les terminaux d'équilibrage 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 doc. Voir ["StorageGRID 11.8 : configurez les certificats d'API S3 et Swift"](#).

Description de la tâche

Par défaut, chaque nœud de stockage est doté d'un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au nœud final de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration terminée sur le serveur, vous devrez peut-être installer le certificat de l'autorité de certification Grid dans le client de l'API S3 que vous utiliserez pour accéder au système, selon 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 d'API S3 personnalisé.

Ajoutez un certificat d'API S3 personnalisé

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (. key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de délivrance de certificat intermédiaire. Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM pour chaque certificat d'API S3 personnalisé téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 suivantes.

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 personnalisé généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 suivantes.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, un certificat signé par l'autorité de certification qui a été chargé ou un certificat personnalisé qui a été généré.



Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

7. Après avoir ajouté un certificat d'API S3 personnalisé, la page de certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé en cours d'utilisation. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Toutefois, vous ne pouvez pas utiliser le certificat d'API S3 par défaut pour un terminal d'équilibreur de charge.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

Lorsque vous restaurez la version par défaut du certificat d'API S3 global, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'API S3 par défaut sera utilisé pour les nouvelles connexions client S3 suivantes 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 d'API S3 personnalisé a été utilisé pour les connexions de terminaux d'équilibrage de charge, une liste s'affiche indiquant les terminaux d'équilibrage de charge qui ne seront plus accessibles à l'aide du certificat d'API S3 par défaut. Accédez à ["Configurer les terminaux de l'équilibreur de charge"](#) pour modifier ou supprimer les points finaux affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Téléchargez ou copiez le certificat d'API S3

Vous pouvez enregistrer ou copier le contenu du certificat de l'API S3 pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le fichier de certificat ou de bundle CA .pem. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Informations associées

- ["UTILISEZ L'API REST S3"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)

Copiez le certificat d'autorité de certification (CA) StorageGRID Grid

StorageGRID utilise une autorité de certification interne pour sécuriser le trafic interne, Ce certificat ne change pas si vous téléchargez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

Si un certificat de serveur personnalisé a été configuré, les applications client doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat de l'autorité de certification depuis le système StorageGRID.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Autorité de certification**

de grille.

2. Dans la section **Certificate PEM**, téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le fichier de certificat .pem.

- a. Sélectionnez **Télécharger le certificat**.
- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Copier le certificat PEM**.
- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui valident rigoureusement le nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP qui utilisent FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le terminal de l'équilibreur de charge.

Avant de commencer

- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, voir ["Configuration de StorageGRID pour FabricPool"](#).

Étapes

1. Configurez également un groupe haute disponibilité (HA) pour FabricPool à utiliser.
2. Créez un terminal d'équilibrage de charge S3 pour FabricPool.

Lorsque vous créez un noeud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA facultatif.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.



Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.

Configurez les certificats clients dans StorageGRID

Les certificats client permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, ce qui fournit un moyen sécurisé aux outils externes de surveillance StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations de certificat dans l'outil externe.

Voir ["Gérer les certificats de sécurité"](#) et ["Configurer des certificats de serveur personnalisés"](#).



Pour garantir que les opérations ne sont pas 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 des clés (KMS) pour protéger les données sur les nœuds d'appliance spécialement configurés, consultez les informations spécifiques à la section ["Téléchargement d'un certificat client KMS"](#).

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Pour configurer un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
 - Si vous avez configuré le certificat de l'interface de gestion StorageGRID, l'autorité de certification, le certificat client et la clé privée sont utilisés pour configurer le certificat de l'interface de gestion.
 - Pour télécharger votre propre certificat, la clé privée du certificat est disponible sur votre ordinateur local.
 - La clé privée doit avoir été enregistrée ou enregistrée au moment de sa création. Si vous ne possédez pas la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.

- Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Pour ajouter le certificat client, utilisez l'une des procédures suivantes :

- [Certificat d'interface de gestion déjà configuré](#)
- [CERTIFICAT client émis](#)
- [Certificat généré par Grid Manager](#)

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification fournie par le client, d'un certificat client et d'une clé privée.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Attach certificates**, téléchargez le certificat de l'interface de gestion.
 - a. Sélectionnez **Télécharger le certificat**.
 - b. Sélectionnez **Browse** et sélectionnez le fichier de certificat de l'interface de gestion (.pem).
 - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

7. [Configurer un outil de surveillance externe](#), Comme Grafana.

CERTIFICAT client émis

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par l'autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes à ["configurez un certificat d'interface de gestion"](#).
2. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Client**.
3. Sélectionnez **Ajouter**.

4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **joindre des certificats**, téléchargez le certificat client, la clé privée et les fichiers de bundle CA :
 - a. Sélectionnez **Télécharger le certificat**.
 - b. Sélectionnez **Browse** et sélectionnez le certificat client, la clé privée et les fichiers de bundle CA (.pem).
 - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Les nouveaux certificats apparaissent sur l'onglet client.

8. [Configurer un outil de surveillance externe](#), Comme Grafana.

Certificat généré par Grid Manager

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction générer certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **joindre des certificats**, sélectionnez **générer un certificat**.
7. Spécifiez les informations de certificat :
 - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
 - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
 - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

Ces extensions définissent l'objectif de la clé contenue dans le certificat.



Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **generate**.

9. sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.



Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

11. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Global**.

12. Sélectionnez **certificat d'interface de gestion**.

13. Sélectionnez **utiliser le certificat personnalisé**.

14. Téléchargez les fichiers `certificate.pem` et `private_key.pem` à partir de [détails du certificat client](#) l'étape. Il n'est pas nécessaire de télécharger le pack CA.

- Sélectionnez **Télécharger le certificat**, puis **Continuer**.
- Télécharger chaque fichier de certificat (`.pem`).
- Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

Le nouveau certificat apparaît sur la page de certificat de l'interface de gestion.

15. [Configurer un outil de surveillance externe](#), Comme Grafana.

configurez un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

- Nom** : saisissez un nom pour la connexion.

StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS client Auth** et avec **CA Cert**.

d. Sous TLS/SSL Auth Details, copiez et collez : +

- Le certificat CA de l'interface de gestion à **CA Cert**
- Le certificat client à **Cert client**
- La clé privée pour **clé client**

e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous au ["Instructions de surveillance de StorageGRID"](#).

Modifier les certificats client

Vous pouvez modifier un certificat de client d'administrateur pour changer son nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat à modifier.

3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**

4. Entrez un nom de certificat.

5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.

6. Sélectionnez **Continuer** pour enregistrer le certificat dans Grid Manager.

Le certificat mis à jour s'affiche dans l'onglet client.

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque celui actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le

tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis sélectionnez une option d'édition.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
- b. Téléchargez le nom du certificat client (.pem).

Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
- c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le certificat mis à jour s'affiche dans l'onglet client.

Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **générer certificat**.
- b. Spécifiez les informations de certificat :

- **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
- **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

Ces extensions définissent l'objectif de la clé contenue dans le certificat.



Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

- c. Sélectionnez **generate**.
- d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.



Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

Téléchargez ou copiez les certificats client

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

- a. Sélectionnez **Télécharger le certificat**.
- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

Copier le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Copier le certificat PEM**.
- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats client

Si vous n'avez plus besoin d'un certificat de client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat à supprimer.
3. Sélectionnez **Supprimer**, puis confirmez.



Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet client, puis sélectionnez **actions > Supprimer**.

Après la suppression d'un certificat, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurez les paramètres de sécurité

Gérez la politique TLS et SSH dans StorageGRID

La règle TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la règle de compatibilité moderne (par défaut), sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.



Certains services StorageGRID n'ont pas été mis à jour pour utiliser le chiffrement inclus dans ces règles.

Avant de commencer

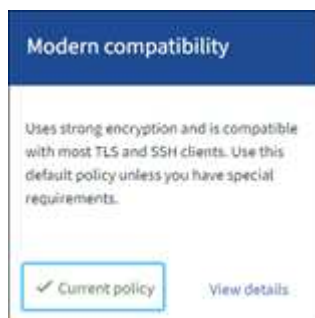
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Sélectionnez une stratégie de sécurité

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.

L'onglet **TLS et SSH policies** affiche les stratégies disponibles. La règle actuellement active est indiquée par une coche verte sur la vignette de la police.



2. Consultez les onglets pour en savoir plus sur les politiques disponibles.

Compatibilité moderne (par défaut)

Utilisez la politique par défaut si vous avez besoin d'un cryptage fort et que vous n'avez pas d'exigences particulières. Cette politique est compatible avec la plupart des clients TLS et SSH.

Compatibilité avec les systèmes existants

Utilisez la politique de compatibilité héritée 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 la politique Critères communs si vous avez besoin d'une certification Critères communs.

Norme FIPS stricte

Utilisez la politique FIPS stricte si vous avez besoin de la certification Critères communs et devez utiliser le NetApp Cryptographic Security Module (NCSM) 3.1.2 ou le module NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au Tenant Manager et au Grid Manager. L'utilisation de cette politique peut réduire les performances.

Le module NCSM 3.1.2 et NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 sont utilisés dans les opérations suivantes :

- NCSM

- Connexions TLS entre les services suivants : ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw et cache-svc
- Connexions TLS entre les clients et le service nginx-gw (points de terminaison de l'équilibreur de charge)
- Connexions TLS entre les clients et le service LDR
- Chiffrement du contenu des objets pour SSE-S3, SSE-C et le paramètre de chiffrement des objets stockés
- Connexions SSH

Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "[Certificat n° A7816](#)".

- Module d'API de chiffrement du noyau NetApp StorageGRID

Le module API de chiffrement du noyau NetApp StorageGRID est présent uniquement sur les plates-formes d'appliances VM et StorageGRID .

- Collection d'entropie
- Chiffrement des nœuds

Remarque : Ce module n'a pas été soumis pour certification.

Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "[Certificat d'entropie n° E223](#)".

Remarque : Après avoir sélectionné cette politique, "[effectuer un redémarrage progressif](#)" pour que tous les nœuds activent le NCSM. Utilisez **Maintenance > Redémarrage progressif** pour lancer et

surveiller les redémarrages.

Personnalisées

Créez une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

Si votre StorageGRID est soumis aux exigences de cryptographie FIPS 140, vous pouvez activer la fonction de mode FIPS pour utiliser le module NCSM 3.1.2 et le module NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 :

- a. Régler le `fipsMode` paramètre à `true`.
- b. Lorsque vous y êtes invité, "[effectuer un redémarrage progressif](#)" pour que tous les nœuds activent les modules de cryptographie. Utilisez **Maintenance > Redémarrage progressif** pour lancer et surveiller les redémarrages.
- c. Sélectionnez **Support > Diagnostics** pour afficher les versions actives du module FIPS.

3. Pour afficher des détails sur les chiffrements, les protocoles et les algorithmes de chaque stratégie, sélectionnez **Afficher les détails**.
4. Pour modifier la stratégie actuelle, sélectionnez **utiliser la stratégie**.

Une coche verte apparaît en regard de **police actuelle** sur la mosaïque de police.

Créez une stratégie de sécurité personnalisée

Vous pouvez créer une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. Dans la mosaïque de la stratégie la plus similaire à la stratégie personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.



3. Dans la mosaïque **Personnaliser la stratégie**, sélectionnez **configurer et utiliser**.
4. Collez le fichier JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **utiliser la stratégie**.

Une coche verte apparaît en regard de **politique actuelle** sur la mosaïque de stratégie personnalisée.

6. Si vous le souhaitez, sélectionnez **Modifier la configuration** pour apporter d'autres modifications à la nouvelle stratégie personnalisée.

Rétablir temporairement la stratégie de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, il se peut que vous ne puissiez pas vous connecter à Grid Manager si la stratégie TLS configurée est incompatible avec ["certificat de serveur configuré"](#).

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Exécutez la commande suivante :

```
restore-default-cipher-configurations
```

3. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.
4. Suivez les étapes de la section [Sélectionnez une stratégie de sécurité](#) pour reconfigurer la stratégie.

Configurer la sécurité du réseau et des objets StorageGRID

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, empêcher certaines requêtes S3 ou autoriser les connexions client aux nœuds de stockage à utiliser le protocole HTTP au lieu du protocole HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données d'objet lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de cryptage AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets récemment acquis sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les objets nouvellement ingérés ne sont pas chiffrés.

Le paramètre de chiffrement des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Pour plus d'informations sur les méthodes de cryptage StorageGRID, reportez-vous à ["Étudiez les méthodes de cryptage StorageGRID"](#) la section .

Empêcher toute modification du client

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option **empêcher la modification du client** est sélectionnée, les demandes suivantes sont refusées.

L'API REST S3

- Demandes DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

Activez HTTP pour les connexions de nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions directes aux nœuds de stockage. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille autre que la production.

Utilisez HTTP pour les connexions 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 (parce que vous pouvez ["configurez chaque point d'extrémité de l'équilibreur de charge"](#) utiliser HTTP ou HTTPS).

Reportez-vous à la section ["Résumé : adresses IP et ports pour les connexions client"](#) pour connaître les ports utilisés par les clients S3 lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **None** (par défaut) si vous ne souhaitez pas que les objets stockés soient cryptés, ou sélectionnez **AES-128** ou **AES-256** pour crypter les objets stockés.
4. Vous pouvez sélectionner **empêcher la modification du client** si vous voulez empêcher les clients S3 de faire des demandes spécifiques.



Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

5. Sélectionnez **Activer HTTP pour les connexions de noeud de stockage** si les clients se connectent directement aux noeuds de stockage et que vous souhaitez utiliser les connexions HTTP.



Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface StorageGRID

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant plus de temps que spécifié et si une trace de pile est incluse dans les réponses d'erreur de l'API.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["Autorisation d'accès racine"](#).

Description de la tâche

La page **Paramètres de sécurité** inclut les paramètres **délai d'inactivité du navigateur** et **trace de pile de l'API de gestion**.

Délai d'inactivité du navigateur dépassé

Indique la durée pendant laquelle le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'inactivité du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique (SSO) est activée pour StorageGRID.

Si 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 ["Comment fonctionne l'authentification unique"](#) .

Trace de la 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 pouvez 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 logiciels internes en cas d'erreurs d'API.

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 la période de temporisation, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai par défaut est de 15 minutes.
 - c. Pour désactiver cette fonction, décochez la case.
 - d. Sélectionnez **Enregistrer**.

Le nouveau paramètre n'affecte pas les utilisateurs qui sont actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'attente prenne effet.

4. Pour modifier le paramètre de trace de pile de l'API de gestion :
 - a. Développez l'accordéon.
 - b. Cochez cette 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 logiciels internes en cas d'erreur d'API.

- c. Sélectionnez **Enregistrer**.

Gérer l'accès SSH externe dans StorageGRID

Gérez l'accès SSH pour le trafic entrant dans la grille en bloquant ou en autorisant l'accès externe. La gestion de l'accès externe SSH n'a pas d'impact sur le trafic entre les nœuds de la grille.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["Autorisation d'accès racine"](#).

Description de la tâche

Pour améliorer la sécurité du système, l'accès SSH externe est bloqué par défaut. Si vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage, autorisez temporairement l'accès externe. Une fois la tâche terminée, bloquez l'accès externe.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **Bloquer SSH**.
3. Utilisez l'option **Bloquer l'accès SSH entrant** pour gérer l'accès SSH externe :
 - a. Cochez la case pour bloquer l'accès (par défaut).
 - b. Décochez la case pour autoriser l'accès.



Nécessite un accès au port 22 entre l'ordinateur portable de service et tous les autres nœuds du réseau. Supprimez l'accès au port 22 une fois la tâche de maintenance terminée.

4. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion des clés

Découvrez les serveurs de gestion des clés dans StorageGRID

Un serveur de gestion des clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à

l'aide du protocole KMIP (Key Management Interoperability Protocol).

StorageGRID prend uniquement en charge certains serveurs de gestion des clés. Pour obtenir la liste des produits et versions pris en charge, utilisez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.

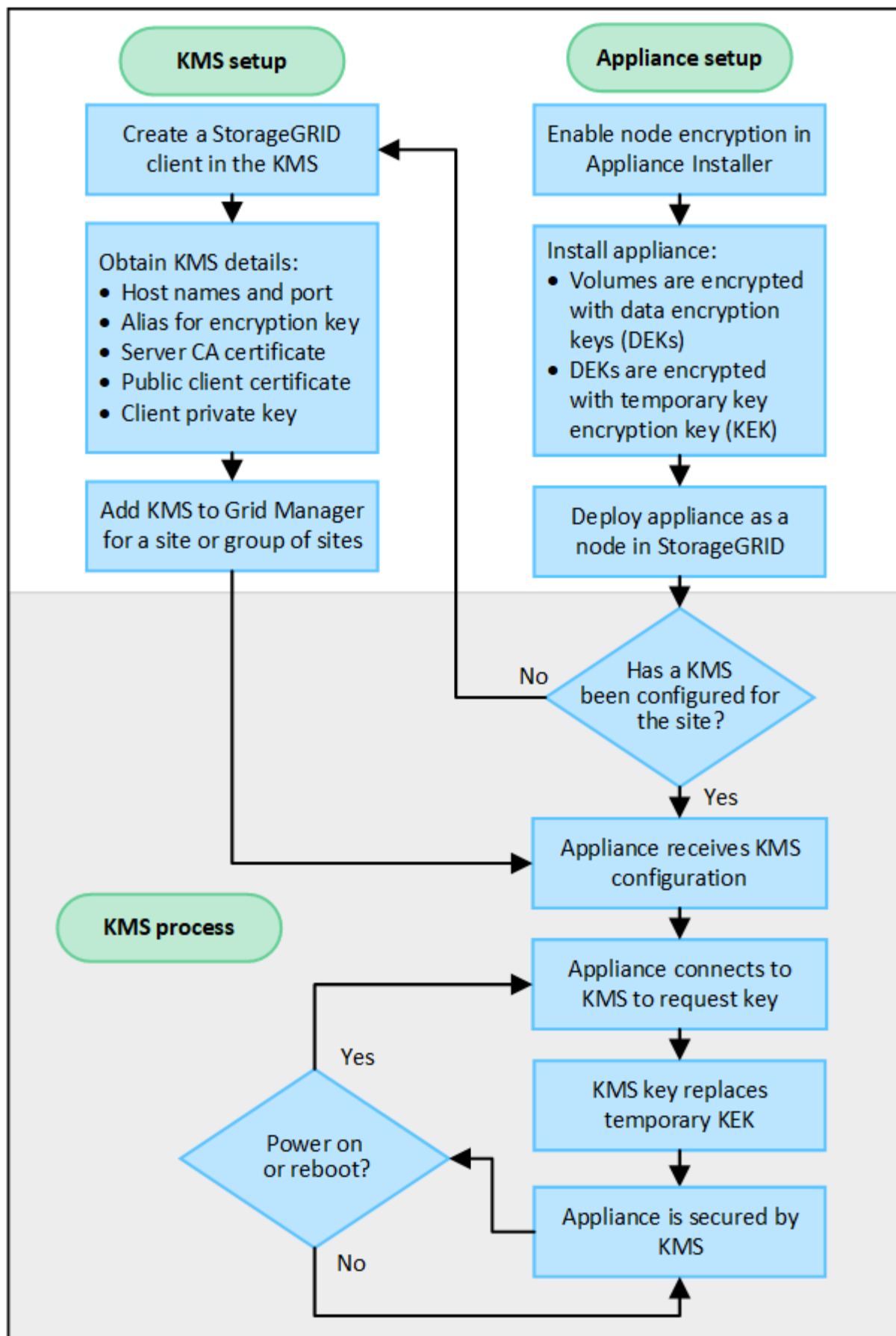


StorageGRID ne crée ni ne gère pas les clés externes utilisées pour chiffrer et décrypter les nœuds des systèmes. Si vous prévoyez d'utiliser un serveur de gestion externe des clés pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et savoir comment gérer les clés de cryptage. Ces instructions ne sont pas uniquement destinées à effectuer des tâches de gestion clés. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion des clés ou contactez le support technique.

Configuration du serveur de gestion des clés et de l'appliance StorageGRID

Avant d'utiliser un serveur de gestion des clés (KMS) afin de sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds pour les nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés est automatique.

L'organigramme présente les étapes générales permettant d'utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.



L'organigramme présente la configuration du KMS et l'appliance en parallèle. Toutefois, vous pouvez

configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenir les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajout d'un serveur de gestion des clés (KMS)"

Configurez l'appareil

La configuration d'un nœud d'appliance pour l'utilisation de KMS comprend les étapes générales suivantes.

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.



Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille, et vous ne pouvez pas utiliser la gestion de clés externe pour les appliances pour lesquelles le chiffrement de nœud n'est pas activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement aléatoire des données (DEK) est attribuée à chaque volume de dispositif, comme suit :
 - Les clés de licence sont utilisées pour chiffrer les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque LUKS (Unified Key Setup) Linux dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
 - Chaque DEK individuel est chiffré par une clé de cryptage principale (KEK). La KEK initiale est une clé temporaire qui chiffre les clés de fin de séjour jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud d'appliance à StorageGRID.

Voir ["Activez le chiffrement de nœud"](#) pour plus de détails.

Processus de chiffrement de la gestion des clés (automatique)

Le chiffrement de la gestion des clés inclut les étapes générales suivantes qui sont automatiquement effectuées.

1. Lorsque vous installez une appliance sur laquelle le chiffrement de nœud est activé dans le grid, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
 - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.

- Si un KMS n'a pas encore été configuré pour le site, les données de l'appliance continuent d'être cryptées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.
2. L'appliance utilise la configuration KMS pour vous connecter au KMS et demander une clé de chiffrement.
 3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé du KMS remplace la KEK temporaire et est maintenant utilisée pour crypter et décrypter les clés de fin de séjour des volumes d'appliance.



Toutes les données qui existent avant que le nœud d'appliance chiffré ne se connecte au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'appliance ne doivent pas être considérés comme protégés de leur retrait du data Center tant que la clé temporaire n'est pas remplacée par la clé de cryptage KMS.

4. Si l'appliance est sous tension ou redémarrée, elle se reconnecte au KMS pour demander la clé. La clé, enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Exigences et considérations relatives au serveur de gestion des clés StorageGRID

Avant de configurer un serveur de gestion des clés externe (KMS), vous devez connaître les considérations et les exigences requises.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge KMIP version 1.4.

["Spécification du protocole d'interopérabilité de gestion des clés version 1.4"](#)

Quelles sont les considérations relatives au réseau ?

Les paramètres de pare-feu réseau doivent permettre à chaque nœud de l'appliance de communiquer via le port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au cluster KMS ou KMS que vous avez configuré pour le site.

Quelles sont les versions de TLS prises en charge ?

Les communications entre les nœuds d'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 des éléments pris en charge par KMS et que ["Règles 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 dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.



Le chiffrement des nœuds ne peut pas être activé après l'ajout d'une appliance à la grille. De plus, vous ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances et les nœuds StorageGRID.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non liés à l'appliance) :

- Nœuds déployés en tant que machines virtuelles
- Nœuds déployés dans les moteurs de mise en conteneurs sur les hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le cryptage en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Dans le cadre d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion des clés dans Grid Manager avant de créer des locataires. Cette commande garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur ces nœuds.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

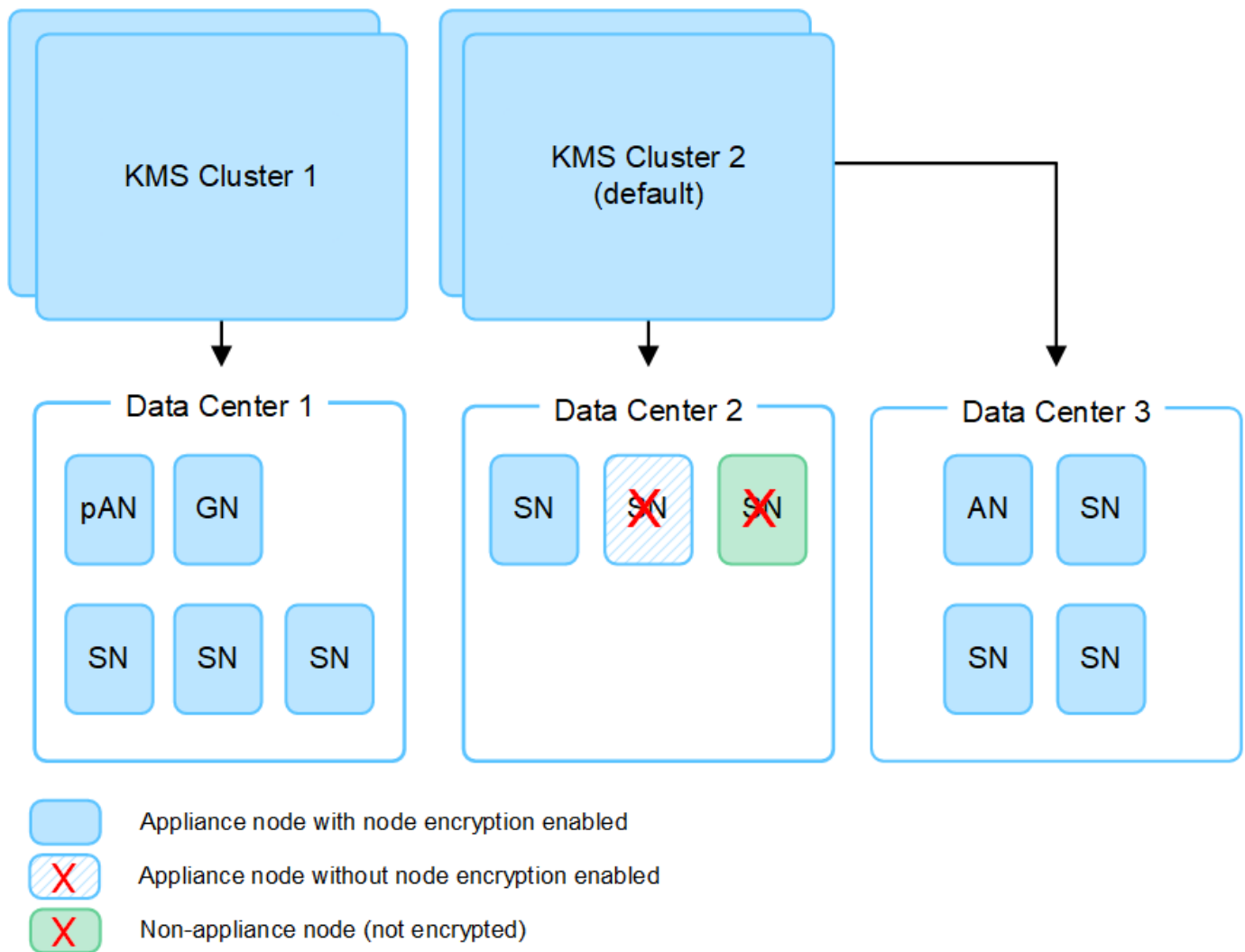
Combien de serveurs de gestion des clés ai-je besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés de chiffrement pour les nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une clé de chiffrement unique aux nœuds d'appliance StorageGRID sur un seul site ou dans un groupe de sites.

StorageGRID prend en charge l'utilisation des clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion des clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée, car il améliore les fonctionnalités de basculement d'une configuration haute disponibilité.

Supposons par exemple que votre système StorageGRID possède trois sites de data Center. Vous pouvez configurer un cluster KMS pour que tous les nœuds d'appliance soient essentiels dans le Data Center 1 et un second cluster KMS pour que ces derniers soient essentiels pour que tous les nœuds d'appliance soient disponibles sur les autres sites. Lorsque vous ajoutez le second cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser de KMS pour les nœuds non liés à l'appliance ou pour les nœuds d'appliance sur lesquels le paramètre **Node Encryption** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que pratique exemplaire en matière de sécurité, vous devez régulièrement ["faites pivoter la clé de cryptage"](#) utiliser chaque KMS configuré.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le redémarrage.
- Si la nouvelle version de clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour une raison quelconque, l'alerte **Echec de la rotation de la clé de chiffrement KMS** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide afin de résoudre cette alerte.

Puis-je réutiliser un nœud d'appliance après chiffrement ?

Si vous devez installer une appliance chiffrée dans un autre système StorageGRID, vous devez d'abord désactiver le nœud de grille pour déplacer les données d'objet vers un autre nœud. Vous pouvez ensuite utiliser le programme d'installation de l'appliance StorageGRID pour ["Effacez la configuration KMS"](#).

L'effacement de la configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID.



Étant donnée l'accès à la clé de chiffrement KMS, toutes les données conservées sur l'appliance ne sont plus accessibles et sont verrouillées en permanence.

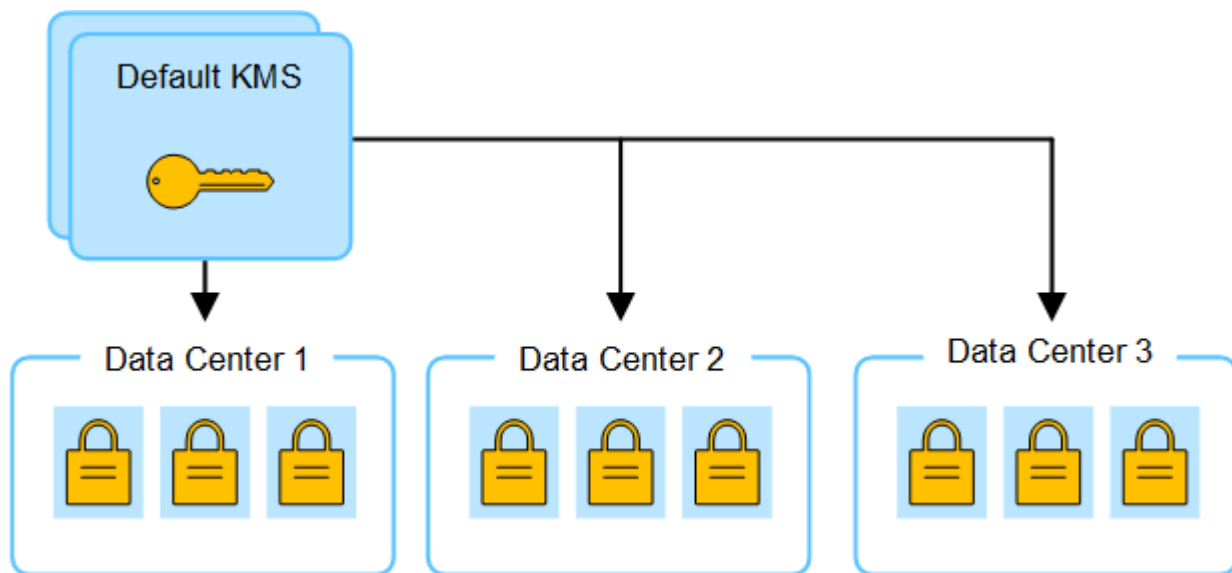
Considérations relatives à la modification du KMS pour un site StorageGRID

Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS vers un autre.

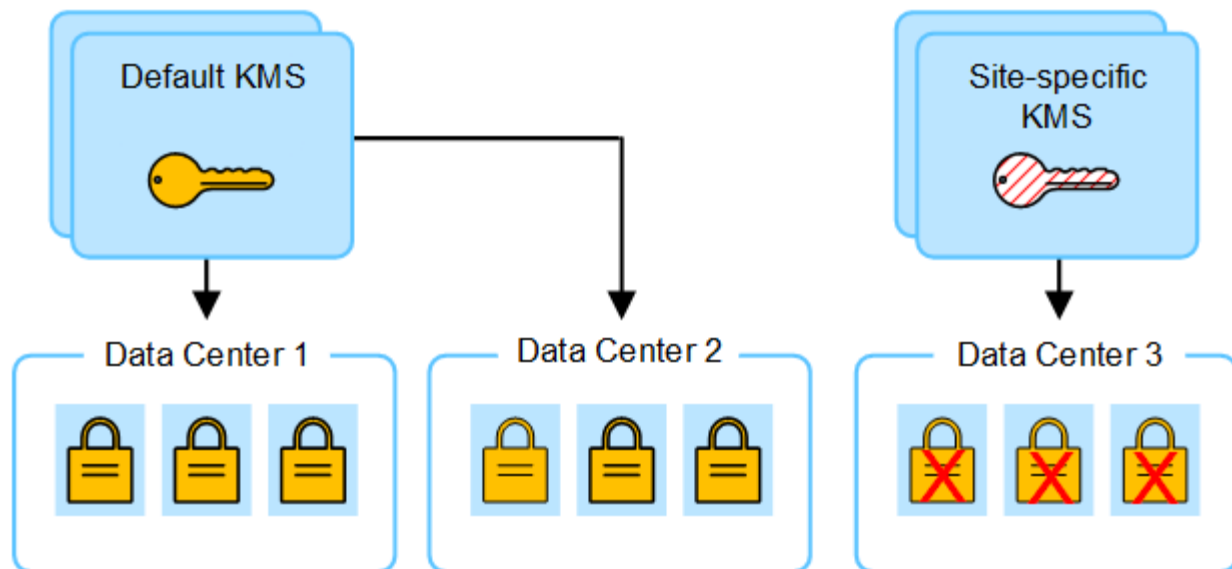
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour décrypter les nœuds de l'appliance chiffrée sur le site.

Par exemple :

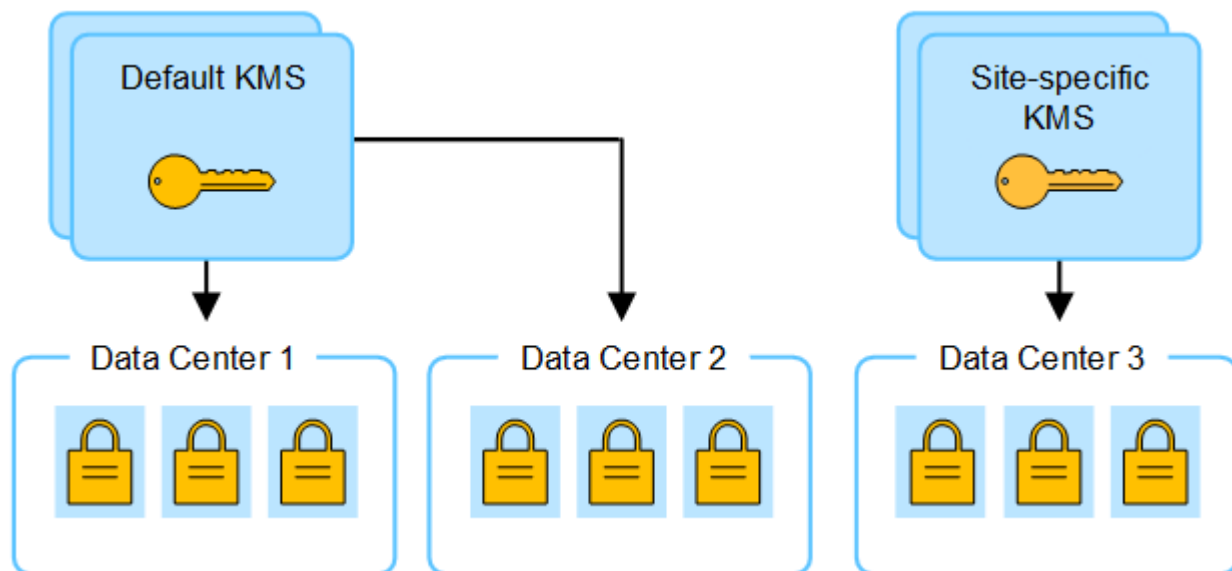
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'appliance sont déjà chiffrés. Une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé appropriée pour décrypter les nœuds de l'appliance sur le data Center 3, afin que ces nœuds puissent être enregistrés dans StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS pour un site.

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ gère clés pour, sélectionnez sites non gérés par un autre KMS (KMS par défaut). Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modification d'un serveur de gestion des clés (KMS)"
Vous avez un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds d'appliance du nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajout d'un serveur de gestion des clés (KMS)"
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. "Ajout d'un serveur de gestion des clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion externe des clés ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.



Ces instructions s'appliquent à Thales CipherTrust Manager et à Hashicorp Vault. Pour obtenir la liste des produits et versions pris en charge, utilisez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque cluster KMS ou KMS que vous souhaitez utiliser.

Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID dans un seul site ou dans un groupe de sites.

2. Créez une clé à l'aide de 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 cluster KMS ou 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 lorsque vous testez et enregistrez après ["téléchargement de certificats client"](#).

3. Notez les informations suivantes pour chaque cluster KMS ou KMS.

Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID :

- Nom d'hôte ou adresse IP pour chaque serveur.
 - Port KMIP utilisé par le KMS.
 - Alias de clé pour la clé de cryptage dans le KMS.
4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

- Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.
- Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.



Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer les mêmes FQDN ou adresses IP dans le champ **Hostname**.

- Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.
5. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés dans StorageGRID

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque cluster KMS ou KMS.

Avant de commencer

- Vous avez examiné le ["considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés"](#).
- Vous avez ["Configuration de StorageGRID en tant que client dans le KMS"](#) et vous avez les informations requises pour chaque cluster KMS ou KMS.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Description de la tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, toutes les appliances chiffrées par nœud dans le grid seront chiffrées par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. Voir ["Considérations relatives à la modification du KMS pour un site"](#) pour plus de détails.

Étape 1 : détails KM

À l'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés), vous fournissez des informations sur le cluster KMS ou KMS.

Étapes

1. Sélectionnez **Configuration > Sécurité > Serveur de gestion des clés**.

La page serveur de gestion des clés s'affiche avec l'onglet Détails de la configuration sélectionné.

2. Sélectionnez **Créer**.

L'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés) s'affiche.

3. Entrez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. 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.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer des serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS gère les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez sites non gérés par un autre KMS (KMS par défaut) pour configurer un KMS par défaut qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. Remarque : Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.

Champ	Description
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. Remarque : le champ Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

- 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**.

Étape 2 : télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat de serveur) de l'assistant Ajouter un serveur de gestion des clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

- A partir de **Étape 2 (Télécharger le certificat de serveur)**, accédez à l'emplacement du certificat de serveur ou du paquet de certificats enregistré.
- Téléchargez le fichier de certificat.

Les métadonnées du certificat de serveur s'affichent.



Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat s'affichent sur son propre onglet.

- Sélectionnez **Continuer**.

étape 3 : téléchargement des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajouter un serveur de gestion des clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

- A partir de **Étape 3 (Téléchargement de certificats client)**, naviguez jusqu'à l'emplacement du certificat client.
- Téléchargez le fichier de certificat client.

Les métadonnées du certificat client s'affichent.

- Accédez à l'emplacement de la clé privée pour le certificat client.
- Téléchargez le fichier de clé privée.
- Sélectionnez **Tester et enregistrer**.

Si aucune clé n'existe, vous êtes invité à en créer une par StorageGRID.

Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les

connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.



Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Test and save**, vérifiez les détails du message, puis sélectionnez **OK**.

Par exemple, vous pourriez recevoir une erreur 422 : entité impossible à traiter si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **forcer l'enregistrement**.



La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

8. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Gérer un serveur de gestion de clés dans StorageGRID

La gestion d'un serveur de gestion des 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 Gestionnaire de grille 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 des clés (KMS) de votre système StorageGRID, y compris les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

1. Sélectionnez **Configuration > Sécurité > Serveur de gestion des clés**.

La page serveur de gestion des clés s'affiche et affiche les informations suivantes :

- L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.
- L'onglet nœuds cryptés répertorie tous les nœuds sur 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	Site StorageGRID associé au KMS Ce champ affiche le nom d'un site StorageGRID spécifique ou sites non gérés par un autre KMS (KMS par défaut) .
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion des clés supplémentaires dans le cluster. Par exemple : 10.10.10.10 and 10.10.10.11 ou 10.10.10.10 and 2 others. Pour afficher tous les noms d'hôte d'une grappe, sélectionnez un KMS et sélectionnez Modifier ou actions > Modifier .

3. Sélectionnez un onglet sur la page de détails KMS pour afficher les informations suivantes :

Onglet	Champ	Description
Détails clés	Nom de la clé	Alias de clé pour le client StorageGRID dans le KMS.
UID de clé	Identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat de serveur	Les métadonnées
Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Contenu du fichier PEM (Privacy Enhanced mail) du certificat.
Certificat client	Les métadonnées	Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. [[clé de rotation]]aussi souvent que requis par les pratiques de sécurité de votre organisation, sélectionnez **clé de rotation**, ou utilisez le logiciel KMS, pour créer une nouvelle version de la clé.

Lorsque la rotation de la clé a réussi, 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 complètement différente.



Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Gérer les certificats

Répondez rapidement à tous les problèmes de certificat de serveur ou de client. Si possible, remplacez les certificats avant qu'ils n'expirent.



Vous devez corriger 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, examinez 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 qu'il est sur le point d'expirer, sélectionnez KMS pour accéder à la page de détails 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 du certificat serveur.
5. Lorsque les alertes **KMS CA Certificate expiration**, **KMS client Certificate expiration** et **KMS Server Certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

StorageGRID peut prendre 30 minutes pour obtenir les mises à jour de l'expiration du certificat. Actualisez votre navigateur Web pour afficher les valeurs actuelles.



Si vous obtenez un état de **l'état du certificat du serveur est inconnu**, assurez-vous que votre KMS permet d'obtenir un certificat du serveur sans exiger 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 **Node Encryption** est activé.

Étapes

1. Sélectionnez **Configuration > Sécurité > Serveur de gestion des clés**.

La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **encrypted nodes**.

L'onglet noeuds cryptés répertorie les noeuds de l'appliance de votre système StorageGRID sur lesquels le paramètre **chiffrement de noeud** est activé.

3. Vérifiez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Nom du nœud d'appliance.
Type de nœud	Le type de nœud : stockage, Administrateur ou passerelle.
Le site	Nom du site StorageGRID sur lequel le nœud est installé.
Nom du KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de la configuration pour ajouter un KMS. "Ajout d'un serveur de gestion des clés (KMS)"
UID de clé	ID unique de la clé de cryptage utilisée pour crypter et décrypter les données sur le nœud de l'appliance. Pour afficher un UID de clé entier, sélectionnez le texte. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de connexion peut prendre plusieurs minutes après la modification de la configuration KMS. Remarque : Rafraîchir votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

- Echec du chargement de la configuration DES KMS
- Erreur de connectivité KMS
- Nom de la clé de cryptage KMS introuvable
- Echec de la rotation de la clé de chiffrement KMS
- La clé KMS n'a pas réussi à décrypter un volume d'appliance
- LES KMS ne sont pas configurés

Effectuez les actions recommandées pour ces alertes.



Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Modifier un KMS

Vous devrez peut-être modifier la configuration d'un serveur de gestion des clés, par exemple si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le ["Considérations relatives à la modification du KMS pour un site"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Configuration > Sécurité > Serveur de gestion des clés**.

La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à modifier, puis sélectionnez **actions > Modifier**.

Vous pouvez également modifier un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Modifier** sur la page de détails KMS.

3. Vous pouvez également mettre à jour les détails dans **Étape 1 (détails KMS)** de l'assistant Modifier un serveur de gestion des 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	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias.

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous ne disposez pas déjà d'un KMS par défaut, sélectionnez éventuellement sites non gérés par un autre KMS (KMS par défaut). Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. Remarque : si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. Remarque : le champ Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.

5. Sélectionnez **Continuer**.

L'étape 2 (Télécharger le certificat de serveur) de l'assistant Modifier un serveur de gestion des clés s'affiche.

6. Si vous devez remplacer le certificat de serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.

7. Sélectionnez **Continuer**.

L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion des clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.

9. Sélectionnez **Tester et enregistrer**.

Les connexions entre le serveur de gestion des clés et tous les nœuds d'appliance chiffrés sur les sites affectés sont testées. Si toutes les connexions de nœud sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion des clés est ajouté à la table de la page Key Management Server.

10. Si un message d'erreur s'affiche, vérifiez les détails du message et sélectionnez **OK**.

Par exemple, vous pouvez recevoir une erreur 422 : entité impossible à traiter si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS, ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **forcer l'enregistrement**.



La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

La configuration KMS est enregistrée.

12. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Suppression d'un serveur de gestion des clés (KMS)

Dans certains cas, vous pouvez supprimer un serveur de gestion des clés. Par exemple, vous pouvez vouloir supprimer un KMS spécifique au site si vous avez désactivé le site.

Avant de commencer

- Vous avez examiné le "[considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Autorisation d'accès racine](#)".

Description de la tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d'appliance lorsque le chiffrement de nœud est activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d'appliance sont activés pour que le chiffrement des nœuds soit activé.

Étapes

1. Sélectionnez **Configuration > Sécurité > Serveur de gestion des clés**.

La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à supprimer, puis sélectionnez **actions > Supprimer**.

Vous pouvez également supprimer un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Supprimer** dans la page de détails KMS.

3. Vérifiez que ce qui suit est vrai :
 - Vous supprimez un KMS spécifique au site pour un site qui n'a aucun nœud d'appliance pour lequel le chiffrement des nœuds est activé.
 - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement des nœuds.
4. Sélectionnez **Oui**.

La configuration KMS est supprimée.

Gérer les paramètres proxy

Configurer un proxy de stockage StorageGRID

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des nœuds finaux externes, tels qu'un nœud final sur Internet.



Les paramètres configurés du proxy de stockage ne s'appliquent pas aux terminaux des services de la plateforme Kafka.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".

Description de la 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 du proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

Laissez ce champ vide pour utiliser le port par défaut du protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

Une fois le proxy de stockage enregistré, il est possible de configurer et de tester de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud.



Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Informations associées

["Ports utilisés pour les communications externes"](#)

Configurez les paramètres du proxy d'administration dans StorageGRID

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, consultez ["Configurez AutoSupport"](#).

Avant de commencer

- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres proxy**.

La page Paramètres proxy s'affiche. Par défaut, l'option stockage est sélectionnée dans le menu de l'onglet.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy Admin**.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

Laissez ces champs vides si votre serveur proxy ne requiert 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 d'administration, sélectionnez **vérifier le certificat proxy**. Téléchargez un paquet CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.



AutoSupport On Demand, E-Series AutoSupport via StorageGRID et la détermination du chemin de mise à jour sur la page mise à niveau StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Une fois le paquet 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.

9. Si vous devez désactiver le proxy admin, décochez la case **Activer le proxy Admin**, puis sélectionnez **Enregistrer**.

Contrôle des pare-feu

Contrôlez l'accès à StorageGRID à un pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne StorageGRID, reportez-vous à la section "[Configurer le pare-feu interne](#)".

Port	Description	Si le port est ouvert...
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. Remarque : le port 443 est également utilisé pour un trafic interne.
8443	Port restreint de Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ou à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder à Grid Manager ou à l'API Grid Management. • Les demandes de contenu interne seront rejetées.



L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

- "[Connectez-vous au Grid Manager](#)"
- "[Créer un compte de locataire](#)"
- "[Communications externes](#)"

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour indiquer si un nœud approuve le trafic entrant provenant du réseau client.

Les paramètres de cet onglet remplacent les paramètres de l'onglet gérer l'accès externe.

- Un nœud avec un réseau client non approuvé accepte uniquement les connexions sur les ports de point final de l'équilibreur de charge configurés sur ce nœud (points finaux globaux, liés à l'interface de nœud et au type de nœud).
- Les ports de point final 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.
- Une fois approuvés, tous les ports ouverts sous l'onglet gérer l'accès externe sont accessibles, ainsi que tous les nœuds finaux d'équilibrage de charge ouverts sur le réseau client.



Les paramètres que vous effectuez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Vérifiez les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous le souhaitez.

Pour configurer les contrôles de pare-feu internes, reportez-vous à la section ["Configurer les contrôles de pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section ["Contrôler l'accès au niveau du pare-feu externe"](#).

Liste d'adresses privilégiées et onglets gérer les accès externes

L'onglet liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP qui ont accès aux ports de la grille fermés. L'onglet gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grid). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour votre grille.



Par défaut, les adresses IP privilégiées n'ont pas d'accès au port de la grille interne.

Exemple 1 : utilisez un hôte de secours pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de secours (un hôte renforcé par la sécurité) pour l'administration du réseau. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.



Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de secours pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : verrouiller les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port. 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 aux ports affectés à Grid Manager et au gestionnaire de locataires (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 à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Une fois votre configuration enregistrée, le port sensible et le service sur ce port sont disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se voient 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 pouvez utiliser la 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 protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les nœuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. C'est-à-dire, par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grille sur tous "ports externes disponibles".

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge. Voir "[Configurer les terminaux de l'équilibreur de charge](#)" et "[Configurer les contrôles de pare-feu](#)".

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous devez effectuer les étapes générales suivantes :

1. À partir de la "[Terminaux d'équilibrage de charge](#)" page, configurez un terminal d'équilibreur de charge pour S3 sur HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez non approuvé pour indiquer que le réseau client sur le nœud passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

Exemple 2 : le nœud de stockage envoie des demandes de services de plateforme S3

Supposons que vous souhaitiez activer le trafic sortant des services de la plateforme S3 à partir d'un nœud de stockage, mais que vous souhaitiez empêcher toute connexion entrante à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans l'onglet réseaux de clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Une fois la configuration enregistrée, le nœud de stockage n'accepte plus le trafic entrant sur le réseau client, mais continue à autoriser les requêtes sortantes vers les destinations de services de plate-forme configurées.

Exemple 3 : limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Procédez comme suit :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet réseau client non approuvé pour configurer le réseau client comme non fiable.
3. Lorsque vous créez un nœud final d'équilibreur de charge dans l'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accèrera.
4. Sélectionnez **Oui** pour réseau client non sécurisé.
5. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Après avoir enregistré votre configuration, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder à Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne de StorageGRID

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 Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez examiné les informations dans "[Gérer les contrôles de pare-feu](#)" et "[Instructions de mise en réseau](#)".

- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des nœuds finaux configurés explicitement, vous avez défini les nœuds finaux de l'équilibreur de charge.



Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les nœuds finaux de l'équilibreur de charge n'ont pas été configurés.

Description de la tâche

StorageGRID comprend un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer des ports ouverts par défaut sur le réseau Grid, le réseau Admin et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant à partir du réseau client et configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre grille à ceux qui sont absolument nécessaires améliore la sécurité de votre grille. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, y compris des exemples, reportez-vous à ["Gérer les contrôles de pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez ["Contrôler l'accès au niveau du pare-feu externe"](#).

Accès aux contrôles de pare-feu

Étapes

1. Sélectionnez **Configuration > Sécurité > Contrôle du pare-feu**.

Les trois onglets de cette page sont décrits dans ["Gérer les contrôles de pare-feu"](#).

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets. Cependant, les modifications de configuration effectuées sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par des paramètres de l'onglet gérer l'accès externe.

Par défaut, les adresses IP privilégiées et les sous-réseaux ne disposent pas d'un accès au grid interne. En outre, les nœuds finaux d'équilibrage de charge et les ports supplémentaires ouverts dans l'onglet liste d'adresses privilégiées sont accessibles même si bloqués dans l'onglet gérer l'accès externe.



Les paramètres de l'onglet Liste d'adresses privilégiées peuvent remplacer ceux de l'onglet Réseau client non approuvé.

Étapes

1. Dans l'onglet liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP que vous souhaitez accorder à l'accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un sous-réseau au format CIDR** pour ajouter des clients privilégiés supplémentaires.



Ajoutez autant d'adresses que possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID**. Reportez-vous à "[Ports internes StorageGRID](#)".



Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet gérer l'accès externe, il est impossible d'accéder au port par une adresse IP non grille à moins que vous n'ajoutiez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.



Les paramètres de l'onglet gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet gérer l'accès externe. Les paramètres de l'onglet réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **gérer l'accès externe**. L'onglet affiche un tableau contenant tous les ports externes (ports accessibles par défaut par les nœuds non GRID) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
 - Utilisez la bascule située en regard de chaque port pour ouvrir ou fermer le port sélectionné.
 - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
 - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.



Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP ait été ajoutée à la liste des adresses privilégiées.



Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en entrant un numéro de port. Vous pouvez entrer un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne "2" s'affichent.

3. Sélectionnez **Enregistrer**

Réseau client non fiable

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points finaux de l'équilibreur de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.



Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration effectuées dans l'onglet **réseau client non approuvé** remplacent les paramètres de l'onglet **gérer l'accès externe**.

Étapes

1. Sélectionnez **réseau client non approuvé**.
2. Dans la section définir les nouveaux nœuds par défaut, spécifiez le paramètre par défaut lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.

- **Approuvé** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
- **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.



Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les terminaux d'équilibrage de charge configurés explicitement ou sur les ports sélectionnés supplémentaires :
 - Sélectionnez **ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste réseau client non approuvé.
 - Sélectionnez **confiance sur les nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste réseau client non approuvé.
 - Utilisez la bascule en regard de chaque nœud pour définir le réseau client comme approuvé ou non fiable pour le nœud sélectionné.

Par exemple, vous pouvez sélectionner **ne plus faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste réseau client non approuvé, puis utiliser la bascule à côté d'un nœud individuel pour ajouter ce nœud à la liste réseau client approuvé.



Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les nœuds disponibles. Utilisez le champ de recherche pour rechercher les paramètres d'un nœud en saisissant son nom. Vous pouvez entrer un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds qui ont la chaîne "GW" comme partie de leur nom sont affichés.

4. 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

Comptes locataires dans StorageGRID

Un compte de 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 doc. Voir ["StorageGRID 11.8 : gestion des locataires"](#).

En tant qu'administrateur du grid, vous créez et gérez les comptes de locataire utilisés par les clients S3 pour stocker et récupérer des objets.

Chaque compte de locataire comprend des groupes, utilisateurs, compartiments S3 et objets fédérés ou locaux.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Cas d'utilisation entreprise** : si vous gérez un système StorageGRID dans une application d'entreprise, vous pourriez vouloir isoler le stockage objet de la grille par les différents départements de votre organisation. Dans ce cas, vous pouvez créer des comptes de tenant pour le département Marketing, le service Customer support, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez utiliser des 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 ["Compartiments S3 et règles de compartiments"](#) pour plus d'informations.

- **Cas d'utilisation de fournisseur de services** : si vous gérez un système StorageGRID en tant que fournisseur de services, vous pouvez isoler le stockage objet de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes de tenant pour la société A, la société B, la société C, etc.

Pour plus d'informations, voir ["Utilisez un compte de locataire"](#).

Comment créer un compte de locataire ?

Utilisez le gestionnaire de grille pour créer un compte de locataire. Lorsque vous créez un compte de locataire, vous spécifiez les informations suivantes :

- Informations de base comprenant le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, vous pouvez activer le paramètre de verrouillage des objets S3 pour le système StorageGRID si les

comptes de locataires S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

À quoi sert le gestionnaire de locataires ?

Une fois le compte de tenant créé, les utilisateurs de tenant peuvent se connecter au gestionnaire de tenant pour effectuer les tâches suivantes :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération de grilles pour la synchronisation des comptes et la réplique inter-grilles
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage



Les locataires S3 peuvent créer et gérer des clés d'accès S3 et des compartiments avec le gestionnaire de locataires. Ils doivent utiliser une application client S3 pour ingérer et gérer les objets. Voir ["UTILISEZ L'API REST S3"](#) pour plus de détails.

Créer un compte locataire StorageGRID

Vous devez créer au moins un compte de locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Les étapes de création d'un compte locataire varient selon que ["fédération des identités"](#) et ["authentification unique"](#) sont configurés et si le compte Grid Manager que vous utilisez pour créer le compte locataire appartient à un groupe d'administrateurs avec l'autorisation d'accès root.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine ou de comptes de locataires"](#).
- Si le compte de tenant utilise le référentiel d'identité qui a été configuré pour Grid Manager et que vous souhaitez accorder l'autorisation d'accès racine au compte de tenant à un groupe fédéré, vous avez importé ce groupe fédéré dans Grid Manager. Vous n'avez pas besoin d'affecter d'autorisations Grid Manager à ce groupe d'administration. Voir ["Gérez les groupes d'administration"](#).
- Si vous souhaitez autoriser un locataire S3 à synchroniser les données de compte et à répliquer les objets du compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles :
 - Vous avez ["configurez la connexion de fédération de grille - effectué"](#).
 - L'état de la connexion est **connecté**.
 - Vous disposez de l'autorisation d'accès racine.
 - Vous avez examiné les considérations relatives à ["gestion des locataires autorisés pour la fédération dans le grid"](#).
 - Si le compte de tenant utilise le référentiel d'identité configuré pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

Lorsque vous créez le tenant, vous sélectionnez ce groupe pour obtenir l'autorisation d'accès racine initiale pour les comptes de tenant source et de destination.



Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

Accéder à l'assistant

Étapes

1. Sélectionnez **Locataires**.
2. Sélectionnez **Créer**.

Entrez les détails

Étapes

1. Entrez les détails du locataire.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lorsque le compte de locataire est créé, il reçoit un ID de compte unique à 20 chiffres.
Description (facultatif)	Une description pour aider à identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grille, vous pouvez utiliser ce champ pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 s'affiche également pour le locataire répliqué dans la grille 2 : « ce locataire a été créé sur la grille 1 ».
Type de client	Doit être S3 .
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire ait un quota de stockage, une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continuer**.

sélectionnez les autorisations

Étapes

1. Si vous le souhaitez, sélectionnez les autorisations de base dont ce locataire doit disposer.



Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisations	Si cette option est sélectionnée...
Autoriser les services de plate-forme	Le locataire peut utiliser des services de plateforme S3 tels que CloudMirror. Voir " Gestion des services de plateforme pour les comptes de locataires S3 ".
Utiliser son propre référentiel d'identité	Le locataire peut configurer et gérer 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 d'API S3 SelectObjectContent pour filtrer et récupérer des données d'objet. Voir "Gérez S3 Select pour les comptes de locataires". Important : les requêtes SelectObjectContent peuvent réduire les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

2. Si vous le souhaitez, sélectionnez les autorisations avancées dont ce locataire doit disposer.

Autorisations	Si cette option est sélectionnée...
Connexion de fédération de grille	Le locataire peut utiliser des connexions de fédération de grille, qui : • Cela permet de synchroniser ce compte locataire ainsi que tous les groupes de locataires, utilisateurs et clés d'accès S3 entre cette grille et les autres grilles des connexions sélectionnées.  Si nécessaire pour des raisons de sécurité ou de conformité, vous pouvez désélectionner Activer la synchronisation des clés d'accès. • Permet à ce locataire de configurer la réplication entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération dans le grid".
Verrouillage d'objet S3	Autoriser le locataire à utiliser des fonctionnalités spécifiques de S3 Object Lock : • Set maximum Retention Period définit la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. • Autoriser le mode de conformité empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégés pendant la période de rétention.

3. Sélectionnez **Continuer**.

Définissez l'accès racine et créez un locataire

Étapes

1. Définissez l'accès racine pour le compte de locataire, selon que votre système StorageGRID utilise ou non la fédération des identités, l'authentification unique (SSO), ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer locataire**.

Un message de réussite s'affiche et le nouveau locataire apparaît sur la page locataires. Pour savoir comment afficher les détails des locataires et surveiller l'activité des locataires, reportez-vous à la section ["Surveillez l'activité des locataires"](#).



L'application des paramètres de locataire sur l'ensemble du grid 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 de fédération de grilles** pour le locataire, vérifiez qu'un locataire identique a bien été répliqué sur l'autre grille de la connexion. Les locataires des deux grilles auront le même ID de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations.



Si vous voyez un message d'erreur indiquant que le compte du locataire a été créé sur cette grille mais n'a pas été synchronisé avec les autres grilles, reportez-vous aux instructions dans ["Dépanner les erreurs de fédération de grille"](#).

Se connecter au locataire (facultatif)

Si nécessaire, vous pouvez vous connecter au nouveau locataire maintenant pour terminer la configuration ou vous pouvez vous connecter ultérieurement au locataire. Les étapes de connexion dépendent si vous êtes connecté à Grid Manager à l'aide du port par défaut (443) ou d'un port restreint. Voir ["Contrôler l'accès au niveau du pare-feu externe"](#).

Connectez-vous dès maintenant

Si vous utilisez...	Procédez comme ça...
Le port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez se connecter en tant que root. Lorsque vous vous connectez, des liens s'affichent pour la configuration des compartiments, de la fédération des identités, des groupes et des utilisateurs. 2. Sélectionnez les liens pour configurer le compte de tenant. Chaque lien ouvre la page correspondante dans le Gestionnaire de locataires. Pour compléter la page, reportez-vous à la "instructions d'utilisation des comptes de tenant".
Le port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez se connecter et entrez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.
Un port restreint	1. Sélectionnez Terminer 2. Sélectionnez Restricted dans la table tenant pour en savoir plus sur l'accès à ce compte de tenant. L'URL du Gestionnaire de locataires a le format suivant : <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ° <i>FQDN_or_Admin_Node_IP</i> Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ° <i>port</i> est le port réservé aux locataires ° <i>20-digit-account-id</i> Est l'ID de compte unique du locataire

Connectez-vous plus tard

Si vous utilisez...	Effectuez l'une d'entre elles...
Orifice 443	• Dans le Gestionnaire de grille, sélectionnez Locataires, puis * Sign in* à droite du nom du locataire. • Entrez l'URL du locataire dans un navigateur Web : <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ° <i>FQDN_or_Admin_Node_IP</i> Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ° <i>20-digit-account-id</i> Est l'ID de compte unique du locataire

Si vous utilisez...	Effectuez l'une d'entre elles...
Un port restreint	- Dans le gestionnaire de grille, sélectionnez Locataires, puis Restreint. - Entrez l'URL du locataire dans un navigateur Web : <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> <i>FQDN_or_Admin_Node_IP</i> Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration <i>port</i> est le port réservé aux locataires <i>20-digit-account-id</i> Est l'ID de compte unique du locataire

Configurez le tenant

Suivez les instructions dans ["Utilisez un compte de locataire"](#) pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les compartiments, les services de plateforme, la synchronisation des comptes et la réplication inter-grilles.

Modifier un compte locataire StorageGRID

Vous pouvez modifier un compte de locataire pour modifier le nom d'affichage, le quota de stockage ou les autorisations de locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine ou de comptes de locataires"](#).



L'application des paramètres de locataire sur l'ensemble du grid peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état du nœud et des opérations Cassandra.

Étapes

- 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](#)

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. Recherchez le compte de locataire à modifier.

Utilisez la zone de recherche pour rechercher un locataire par nom ou ID locataire.

3. Sélectionnez le locataire. Vous pouvez effectuer l'une des opérations suivantes :

- Cochez la case du locataire, puis sélectionnez **actions > Modifier**.
- Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **Modifier**.

4. Si vous le souhaitez, modifiez les valeurs de ces champs :

- **Nom**
- **Description**
- **Quota de stockage**

5. Sélectionnez **Continuer**.

6. Sélectionnez ou désélectionnez les autorisations pour le compte de tenant.

- Si vous désactivez **Platform Services** pour un locataire qui les utilise déjà, les services qu'ils ont configurés pour leurs compartiments S3 cessent de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il peut toujours stocker les objets dans le compartiment, mais les copies de ces objets ne sont plus effectuées dans le compartiment S3 externe qu'ils ont configuré en tant que terminal. Voir "[Gestion des services de plateforme pour les comptes de locataires S3](#)".
- Modifiez le paramètre de **Use own Identity source** pour déterminer si le compte de tenant utilisera son propre référentiel d'identité ou le référentiel d'identité configuré pour le gestionnaire de grille.

Si **utiliser le propre référentiel d'identité** est :

- Désactivé et sélectionné, le locataire a déjà activé son propre référentiel d'identité. Un locataire doit désactiver son référentiel d'identité avant de pouvoir utiliser le référentiel d'identité configuré pour Grid Manager.
- Désactivé et non sélectionné, SSO est activé pour le système StorageGRID. Le locataire doit utiliser le référentiel d'identité qui a été configuré pour Grid Manager.

- Sélectionnez ou désélectionnez l'autorisation **Autoriser S3 Select** selon les besoins. Voir "[Gérez S3 Select pour les comptes de locataires](#)".
- Pour supprimer l'autorisation **utiliser la connexion de fédération de grille** :
 - i. Sélectionnez l'onglet **Fédération Grid** sur la page des détails du locataire.
 - ii. Sélectionnez la connexion que vous souhaitez supprimer.
 - iii. Sélectionnez **Supprimer l'autorisation**.
- Pour ajouter l'autorisation **utiliser la connexion de fédération de grille** :
 - i. Sélectionnez l'onglet **Grid federation**.
 - ii. Cochez la case **utiliser la connexion de fédération de grille**.
 - iii. Si vous le souhaitez, sélectionnez **Cloner les utilisateurs et groupes locaux existants** pour les cloner dans 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 dernière opération de clonage.



Si nécessaire pour des raisons de sécurité ou de conformité, vous pouvez désélectionner **Activer la synchronisation des clés d'accès**.

- Pour définir une période de rétention maximale ou autoriser le mode de conformité :



Le verrouillage d'objet S3 doit être activé sur la grille pour que vous puissiez utiliser ces paramètres.

- i. Sélectionnez l'onglet **S3 Object Lock**.
- ii. Pour **définir la période de rétention maximale**, entrez une valeur et sélectionnez la période dans le menu déroulant.
- iii. Pour **Autoriser le mode de conformité**, cochez la case.

Modifier le mot de passe de l'utilisateur root local d'un locataire StorageGRID

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si celui-ci est verrouillé hors du compte.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Description de la tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte de locataire. Pour effectuer des tâches utilisateur racine, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès racine pour le locataire.

Étapes

1. Sélectionnez **Locataires**.

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](#)

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	→ 📄

- Sélectionnez le compte locataire. Vous pouvez effectuer l'une des opérations suivantes :
 - Cochez la case du locataire, puis sélectionnez **actions** > **Modifier le mot de passe root**.
 - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **actions** > **Modifier le mot de passe root**.
- Saisissez le nouveau mot de passe du compte de tenant.
- Sélectionnez **Enregistrer**.

Supprimer un compte locataire StorageGRID

Vous pouvez supprimer un compte de tenant si vous souhaitez supprimer définitivement l'accès du tenant au système.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez supprimé tous les compartiments S3 et tous les objets associés au compte de locataire.
- Si le locataire est autorisé à utiliser les connexions de fédération de grilles, vous avez pris connaissance des points à prendre en ["Suppression d'un locataire avec l'autorisation utiliser la connexion de fédération de grille"](#) compte. Les suppressions sont synchronisées, donc si un locataire est supprimé sur une grille, il sera supprimé sur toutes les grilles sélectionnées.

Étapes

- Sélectionnez **Locataires**.
- Recherchez le ou les comptes de tenant que vous souhaitez supprimer.

Utilisez la zone de recherche pour rechercher un locataire par nom ou ID locataire.

- Pour supprimer plusieurs locataires, cochez les cases et sélectionnez **actions** > **Supprimer**.
- Pour supprimer un seul locataire, effectuez l'une des opérations suivantes :

- Cochez la case et sélectionnez **actions > Supprimer**.
- Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **actions > Supprimer**.

5. Sélectionnez **Oui**.

Gestion des services de plateforme

Découvrez les services de la plateforme StorageGRID

Les services de plateforme incluent la réplication CloudMirror, les notifications d'événement et le service d'intégration de la recherche.

Si vous activez des services de plateforme pour les comptes de locataires S3, vous devez configurer votre grid de manière à ce que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Les services de plateforme ne sont pas pris en charge pour ["seaux de branches"](#) .

Réplication CloudMirror

Le service de réplication StorageGRID CloudMirror est utilisé pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir ["Comparez la réplication entre les grilles et la réplication CloudMirror"](#).

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, à un point de terminaison webhook ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.



Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Service d'intégration de la recherche

Le service d'intégration de la recherche permet d'envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié pour une recherche ou une analyse des métadonnées à l'aide du service externe.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.



Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Les services de plateforme permettent aux locataires d'utiliser des ressources de stockage externes, des services de notification et des services de recherche ou d'analyse avec leurs données. Étant donné que l'emplacement cible des services de plateforme ne fait généralement pas partie de votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Dans ce cas, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes de tenant. Vous devez également configurer votre réseau de sorte que les messages de services de plate-forme générés par les locataires puissent atteindre leurs destinations.

Recommandations relatives à l'utilisation des services de plate-forme

Avant d'utiliser les services de plate-forme, tenez compte des recommandations suivantes :

- Si le contrôle de versions et la réplication CloudMirror sont activés pour un compartiment S3 dans le système StorageGRID, vous devez également activer la gestion des versions du compartiment S3 pour le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Les demandes adressées à un point final qui ne peut pas être terminé seront mises en file d'attente pour un maximum de 500,000 demandes. Cette limite est également partagée entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500,000 afin que les locataires nouvellement créés ne soient pas pénalisés injustement.

Informations associées

- ["Gestion des services de plateforme"](#)
- ["Configurez les paramètres du proxy de stockage"](#)
- ["Surveillez StorageGRID"](#)

Réseau et ports pour les services de plateforme StorageGRID

Si vous autorisez un locataire S3 à utiliser des services de plateforme, vous devez configurer la mise en réseau pour le grid de manière à ce que les messages des services de plateforme puissent être envoyés vers leur destination.

Lorsque vous créez ou mettez à jour le compte de locataire, vous pouvez activer des services de plateforme pour un compte de locataire S3. Si les services de plateforme sont activés, le locataire peut créer des terminaux qui servent de destination à la réplication CloudMirror, à la notification d'événement ou aux messages d'intégration de recherche à partir de ses compartiments S3. Ces messages de services de plateforme sont envoyés depuis les nœuds de stockage qui exécutent le service ADC vers les terminaux de destination.

Par exemple, les locataires peuvent configurer les types de terminaux de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Application locale qui prend en charge la réception des messages Amazon simple notification Service

- Cluster Kafka hébergé localement
- Un point de terminaison webhook externe ou hébergé localement qui prend en charge les requêtes de notification HTTP POST.

Ce point de terminaison peut être hébergé sur divers serveurs Web, frameworks ou outils de traitement de données tels que Fluentd.

- Un compartiment S3 hébergé localement sur la même instance d'StorageGRID ou sur une autre instance
- Un terminal externe, tel qu'un terminal sur Amazon Web Services.

Pour vous assurer que les messages des services de plate-forme peuvent être envoyés, vous devez configurer le réseau ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer des messages de services de plate-forme aux nœuds finaux de destination.

Par défaut, les messages des services de plate-forme sont envoyés sur les ports suivants :

- **80** : pour les URI de nœud final commençant par http (la plupart des nœuds finaux)
- **443** : pour les URI de nœud final commençant par https (la plupart des nœuds finaux)
- **9092** : pour les URI de nœud final commençant par http ou https (nœuds finaux Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un nœud final.



Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, des messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Vérifiez que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le terminal.

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

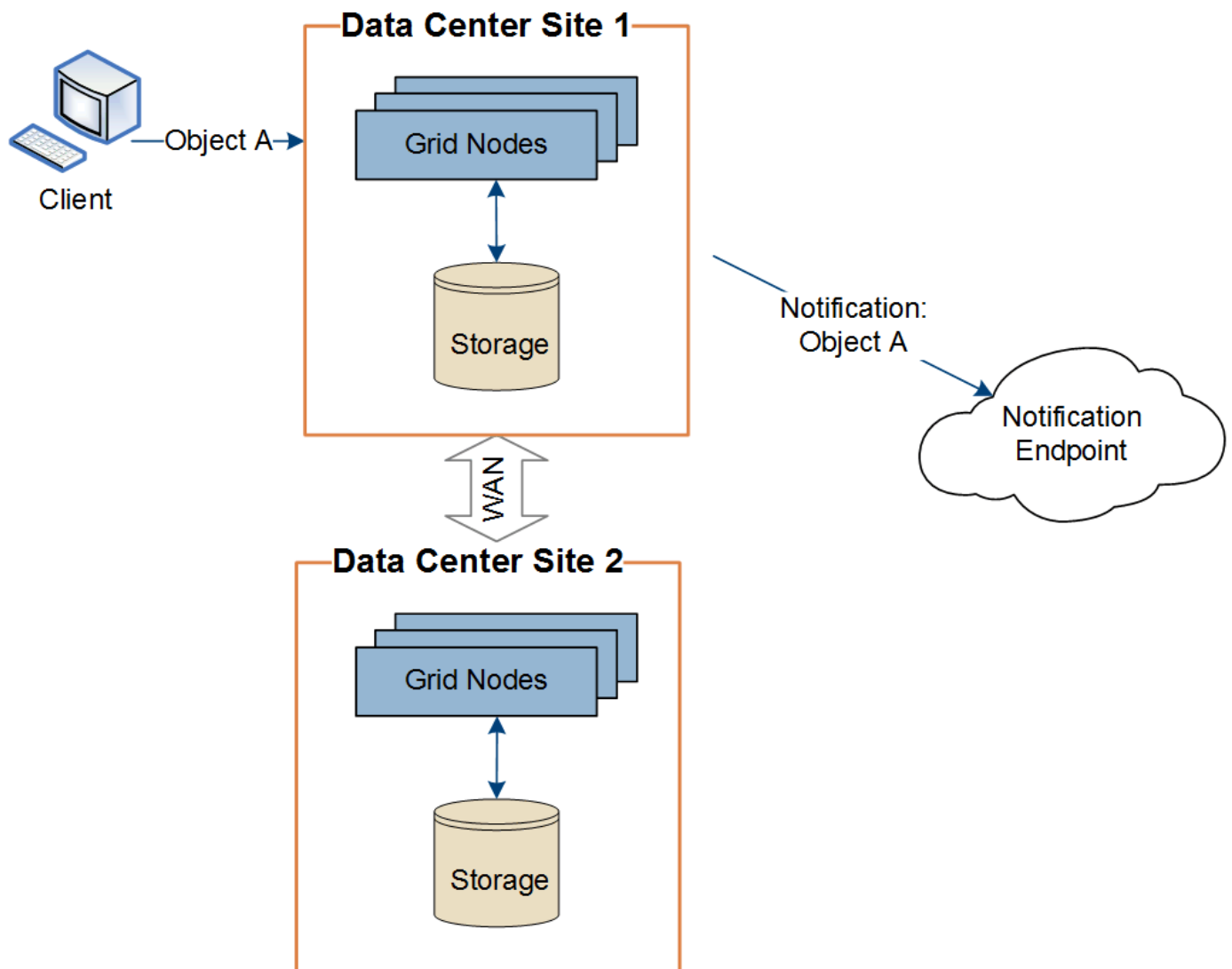
Informations associées

- "[Utilisez un compte de locataire](#)"
- "[Ports utilisés pour les communications externes](#)"

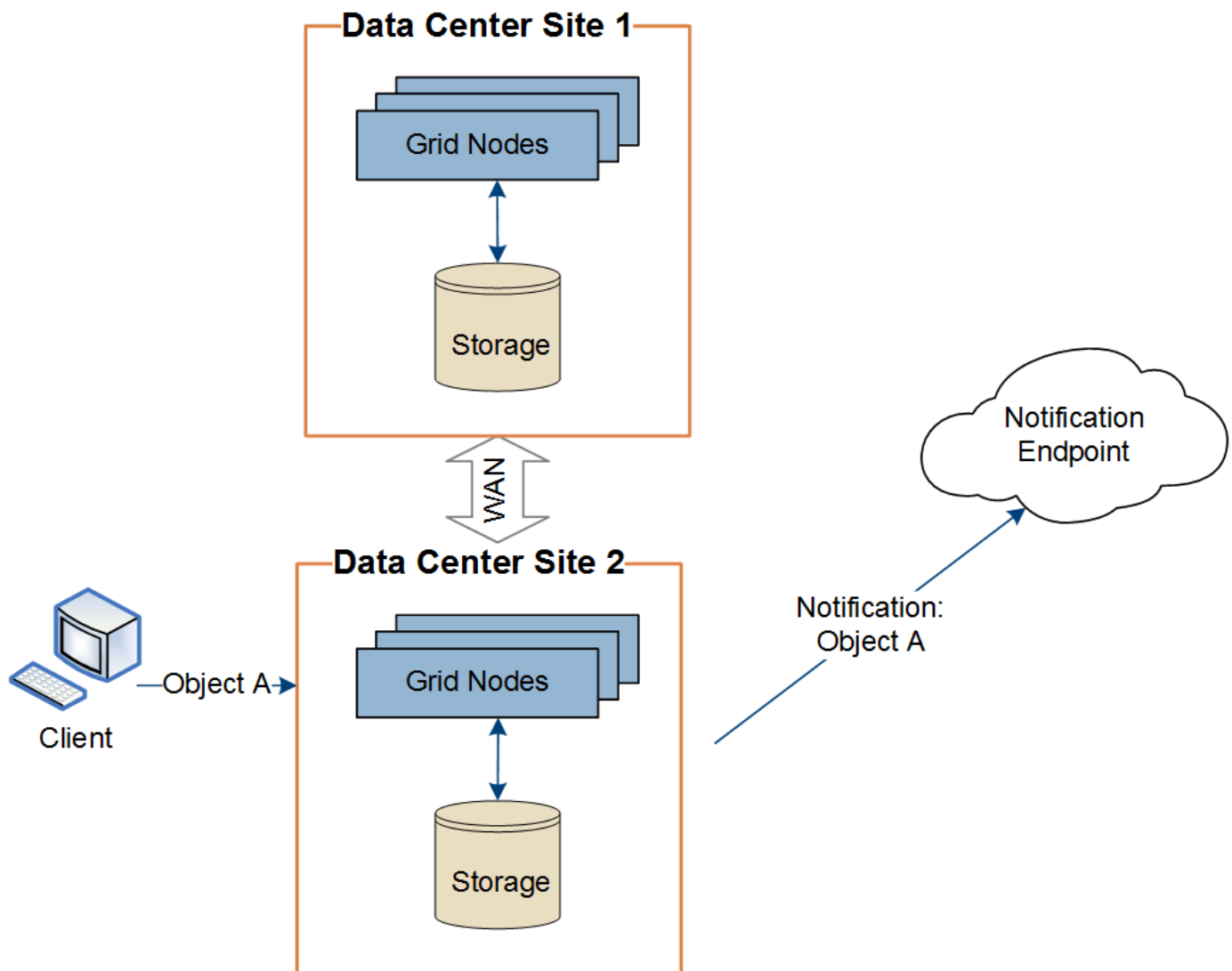
Livraison par site des messages des services de plateforme StorageGRID

Toutes les opérations de services de plateforme sont réalisées sur une base par site.

C'est-à-dire que si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle sur le site de Data Center 1, la notification concernant cette action est déclenchée et envoyée depuis le site de Data Center 1.



Si le client exécute ensuite une opération de suppression d'API S3 sur ce même objet à partir du site du centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis le site du centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de plate-forme puissent être transmis à leurs destinations.

Dépanner les services de plateforme StorageGRID

Les points de terminaison utilisés dans les services de la plateforme sont créés et gérés par les utilisateurs locataires dans le Tenant Manager. Cependant, si un locataire rencontre des difficultés pour configurer ou utiliser les services de la plateforme, vous pouvez utiliser le Grid Manager pour aider à résoudre le problème.

Problèmes liés aux nouveaux terminaux

Avant qu'un locataire ne puisse utiliser les services de plateforme, il doit créer un ou plusieurs terminaux à l'aide du Gestionnaire des locataires. Chaque terminal représente une destination externe pour un service de plateforme, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, une rubrique Amazon simple notification Service, une rubrique Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque noeud final comprend à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un noeud final, le système StorageGRID valide que ce dernier existe et qu'il peut être atteint à l'aide des identifiants spécifiés. La connexion au noeud final est validée à partir d'un noeud sur chaque

site.

Si la validation du noeud final échoue, un message d'erreur explique pourquoi la validation du noeud final a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer de créer à nouveau le noeud final.



La création du terminal échoue si les services de plateforme ne sont pas activés pour le compte de locataire.

Problèmes avec les terminaux existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un noeud final existant, un message s'affiche sur le tableau de bord dans le Gestionnaire de locataires.



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 examiner 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 l'icône  se sont produites 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 le support technique peut utiliser cet ID pour trouver des informations plus détaillées sur l'erreur dans bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un "proxy de stockage" entre les 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.

Déterminez si une erreur s'est produite

Si des erreurs de nœud final se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page nœuds finaux pour obtenir plus de détails sur l'erreur.

Échec des opérations client

Certains problèmes de service de plateforme peuvent entraîner l'échec des opérations client dans le compartiment S3. Par exemple, les opérations client S3 échouent si le service RSM (Replicated State machine) interne s'arrête ou s'il y a trop de messages de services de plate-forme en file d'attente pour la livraison.

Pour vérifier l'état des services :

1. Sélectionnez **Nœuds > site > Nœud de stockage > Aperçu**.
2. Vérifiez les alertes actives dans le tableau Alertes.
3. Résolvez toutes les alertes actives. Si nécessaire, contactez le support technique.

Erreurs récupérables et récupérables du point final

Une fois les nœuds finaux créés, des erreurs de demande de service de plate-forme peuvent se produire pour diverses raisons. Certaines erreurs peuvent être récupérées avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent se produire pour les raisons suivantes :

- Les informations d'identification de l'utilisateur ont été supprimées ou ont expiré.
- Le bucket de destination n'existe pas.
- La notification ne peut pas être remise.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plate-forme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, des erreurs irrécupérables peuvent se produire pour les raisons suivantes :

- Le point de terminaison est supprimé.
- Une destination de point de terminaison webhook répond à une demande de notification avec un 400 `Bad Request` erreur.

Si StorageGRID rencontre une erreur de point final irrécupérable :

- Dans Grid Manager, accédez à **support > Tools > Metrics > Grafana > Platform Services Overview** pour afficher les détails de l'erreur.
- Dans le Gestionnaire de locataires, accédez à **STORAGE (S3) > Platform Services Endpoints** pour afficher les détails de l'erreur.

- Vérifier si le `/var/local/log/bycast-err.log` présente des erreurs. Les nœuds de stockage disposant du service ADC contiennent ce fichier journal.

Les messages des services de plateforme ne peuvent pas être transmis

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.

Recherchez les alertes associées.

Des performances plus lentes pour les demandes de services de plateforme

Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le nœud final de destination.

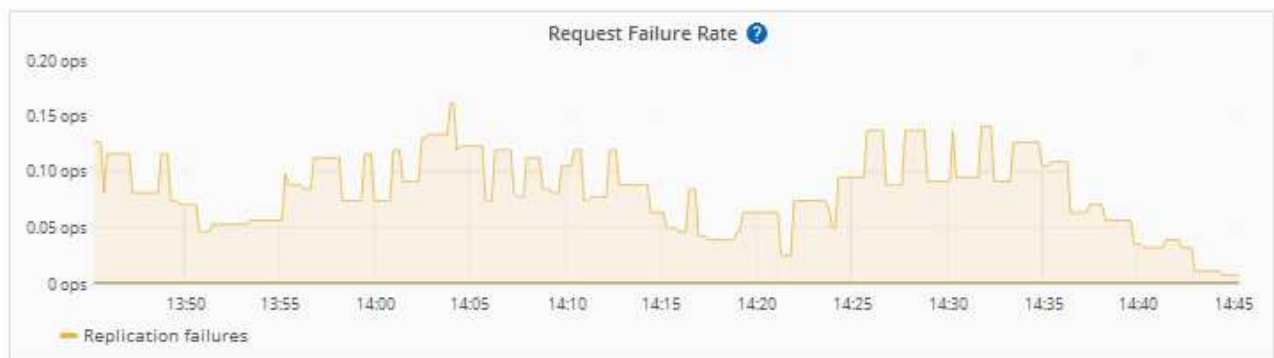
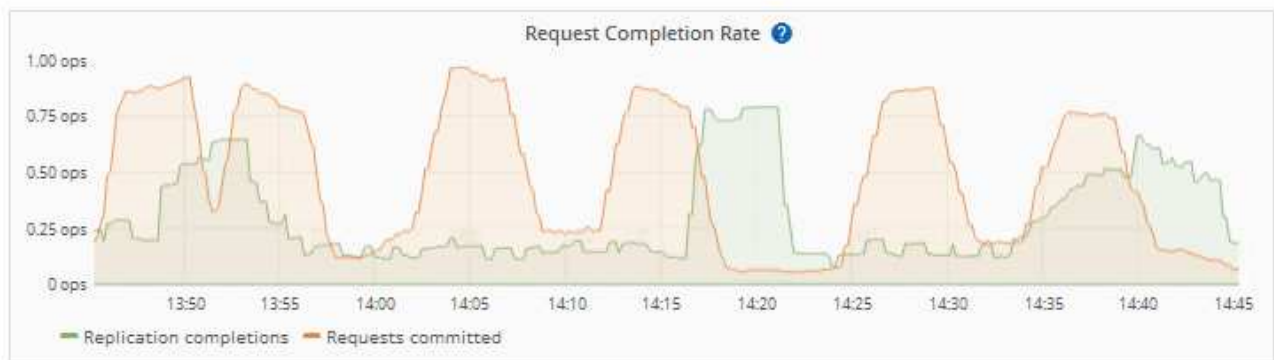
Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'arnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.

Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d'échec de la demande pour les services de plate-forme :

1. Sélectionnez **Nœuds**.
2. Sélectionnez **site > Platform Services**.
3. Afficher le tableau des taux d'erreur de demande.



Alerte de services de plate-forme non disponibles

L'alerte **Platform services unavailable** indique qu'aucune opération de service de plate-forme ne peut être effectuée sur un site car trop de nœuds de stockage avec le service RSM sont en cours d'exécution ou indisponibles.

Le service RSM garantit que les demandes de service de plate-forme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, déterminez quels nœuds de stockage du site incluent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui incluent également le service ADC.) Ensuite, assurez-vous 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 toute demande de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les terminaux des services de plateforme

Pour plus d'informations, voir ["Utiliser un compte locataire ; dépanner les terminaux des services de plateforme"](#).

Informations associées

["Dépanner le système StorageGRID"](#)

Gérer S3 Select pour les comptes locataires dans StorageGRID

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes `SelectObjectContent` sur des objets individuels.

S3 Select constitue un moyen efficace d'effectuer des recherches dans de vastes volumes de données sans avoir à déployer une base de données et les ressources associées pour activer les recherches. Il réduit également le coût et la latence liés à la récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser les requêtes `SelectObjectContent` pour filtrer et récupérer uniquement les données nécessaires à partir d'un objet. L'implémentation d'StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et configuration requise pour l'utilisation de S3 Select

Exigences d'administration du grid

L'administrateur du grid doit autoriser les locataires S3 Select. Sélectionnez **Autoriser la sélection S3** lorsque ["création d'un locataire"](#) ou ["modification d'un locataire"](#).

Exigences de format d'objet

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets parquet :
 - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets parquet.
 - S3 Select ne prend pas en charge la sortie parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
 - La taille maximale du groupe de lignes non compressées est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
 - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.

Exigences relatives aux terminaux

La demande SelectObjectContent doit être envoyée à un ["Terminal d'équilibrage de charge StorageGRID"](#).

Les nœuds d'administration et de passerelle utilisés par le nœud final doivent être l'un des suivants :

- Nœud d'appliance de services
- Nœud logiciel basé sur VMware
- Nœud bare Metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.



SelectObjectContent les demandes peuvent réduire les performances d'équilibrage de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

Voir la ["Instructions d'utilisation de S3 Select"](#).

Pour voir ["Graphiques 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 à StorageGRID

En tant qu'administrateur du grid, vous gérez les options de configuration qui contrôlent la façon dont les applications client S3 se connectent à votre système StorageGRID pour stocker et récupérer les données.



Les détails SWIFT ont été supprimés de cette version du site doc. Voir ["StorageGRID 11.8 : configurez les connexions client S3 et Swift"](#).

Tâches de configuration

1. Effectuez les tâches requises dans StorageGRID, en fonction de la façon dont l'application client se connecte à StorageGRID.

Tâches requises

Vous devez obtenir :

- Adresses IP
- Noms de domaine
- Certificat SSL

Tâches facultatives

Éventuellement, configurer :

- fédération des identités
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez utiliser l'assistant d'installation S3 ou configurer chaque entité StorageGRID manuellement. +

Utilisation de l'assistant d'installation S3

Suivez les étapes de l'assistant d'installation de S3.

Configurer manuellement

1. Créer un groupe haute disponibilité
2. Créer un noeud final d'équilibreur de charge
3. Créer un compte de locataire
4. Créez un compartiment et des clés d'accès
5. Configuration de la règle et de la règle 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 supplémentaire de l'application.

2. Effectuez des tâches continues dans l'application et dans StorageGRID afin de gérer et de surveiller le stockage objet au fil du temps.

Informations nécessaires pour joindre StorageGRID à une application client

Avant de connecter StorageGRID à une application client S3, vous devez effectuer les étapes de configuration dans StorageGRID et obtenir une certaine valeur.

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)	Groupe StorageGRID > HA	Entrée DNS
Port	StorageGRID > terminal de l'équilibreur de charge	Application client
Certificat SSL	StorageGRID > terminal de l'équilibreur de charge	Application client
Nom du serveur (FQDN)	StorageGRID > terminal de l'équilibreur de charge	• Application client • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > locataire et compartiment	Application client
Nom du compartiment/conteneur	StorageGRID > locataire et compartiment	Application client

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez effectuer l'une des opérations suivantes pour obtenir les informations dont vous avez besoin :

- **Utilisez le "Assistant d'installation S3"**. L'assistant d'installation S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser pour configurer l'application S3. L'assistant vous guide tout au long des étapes requises et vous aide à vous assurer que vos paramètres sont conformes aux bonnes pratiques de StorageGRID.



Si vous configurez une application S3, il est recommandé d'utiliser l'assistant d'installation S3, sauf si vous savez que vous disposez d'exigences spéciales, faute de quoi votre implémentation nécessitera une personnalisation importante.

- **Utilisez le "Assistant d'installation FabricPool"**. À l'instar de l'assistant d'installation de S3, l'assistant d'installation de FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser pour configurer un Tier cloud FabricPool dans ONTAP.



Si vous prévoyez d'utiliser StorageGRID en tant que système de stockage objet pour un niveau cloud FabricPool, il est recommandé d'utiliser l'assistant d'installation FabricPool, sauf si vous disposez d'une configuration spécifique ou si votre implémentation nécessite une personnalisation importante.

- **Configurer les éléments manuellement.** Si vous vous connectez à une application S3 et que vous préférez ne pas utiliser l'assistant d'installation S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Voici la procédure à suivre :
 - a. Configurez le groupe haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir ["Configurez les groupes haute disponibilité"](#).
 - b. Créez le terminal d'équilibrage de charge que l'application S3 utilisera. Voir ["Configurer les terminaux de l'équilibreur de charge"](#).

- c. Créez le compte locataire que l'application S3 utilisera. Voir ["Créez un compte de locataire"](#).
- d. Pour un locataire S3, connectez-vous au compte du locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accèrera à l'application. Voir ["Créez vos propres clés d'accès"](#).
- e. Créez un ou plusieurs compartiments S3 dans le compte de locataire. Pour S3, voir ["Créer un compartiment S3"](#).
- f. Pour ajouter des instructions de placement spécifiques pour les objets appartenant au nouveau locataire ou compartiment/conteneur, créez une règle ILM et activez une nouvelle règle ILM pour utiliser cette règle. Voir ["Création d'une règle ILM"](#) et ["Création de la règle ILM"](#).

Sécurité des clients S3 dans StorageGRID

Les comptes de locataires StorageGRID utilisent les applications client S3 pour enregistrer les données d'objet dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications client.

Récapitulatif

La liste ci-dessous résume la mise en œuvre de la sécurité pour l'API REST S3 :

Sécurité de la connexion

TLS

Authentification du serveur

Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur

Authentification client

ID de clé d'accès de compte S3 et clé d'accès secrète

Autorisation du client

Propriété des compartiments et toutes les règles de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications client

Les applications client S3 peuvent se connecter au service Load Balancer sur des nœuds de passerelle ou des nœuds d'administration ou directement sur les nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, en fonction de la façon dont vous ["configurez le nœud final de l'équilibreur de charge"](#).

Le protocole HTTPS fournit une communication sécurisée et cryptée TLS. Il est recommandé de le faire. Vous devez associer un certificat de sécurité au nœud final.

HTTP fournit une communication non chiffrée moins sécurisée 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 non chiffrée moins sécurisée, mais peut être facultatif ["activé"](#) pour les

grilles de non-production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir "[En-têtes d'authentification HTTP](#)" à StorageGRID pour effectuer les opérations de l'API REST.

Certificats de sécurité et applications client

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles utilisent le certificat configuré pour le nœud final de l'équilibreur de charge. Chaque nœud final de l'équilibreur de charge possède son propre certificat—soit un certificat de serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat généré par l'administrateur de la grille dans StorageGRID lors de la configuration du nœud final.

Voir "[Considérations relatives à l'équilibrage de charge](#)".

- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille. Voir "[Ajoutez un certificat d'API S3 personnalisé](#)".

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de cryptage 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 supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utilisation de l'assistant d'installation S3

Considérations et exigences de l'assistant de configuration StorageGRID S3

À l'aide de l'assistant d'installation S3, vous pouvez configurer StorageGRID en tant que système de stockage objet d'une application S3.

Utilisation de l'assistant d'installation S3

L'assistant d'installation S3 vous guide à chaque étape de la configuration d'StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'assistant, vous téléchargez des fichiers que vous pouvez utiliser

pour saisir des valeurs dans l'application S3. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID.

Si vous disposez du "[Autorisation d'accès racine](#)", vous pouvez compléter l'assistant d'installation S3 lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement. Selon vos besoins, vous pouvez également configurer une partie ou la totalité des éléments requis manuellement, puis utiliser l'assistant pour assembler les valeurs dont une application S3 a besoin.

Avant d'utiliser l'assistant

Avant d'utiliser l'assistant, vérifiez que vous avez terminé ces conditions préalables.

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité, vous savez à quels nœuds l'application S3 se connectera et à quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs entrer pour le CIDR de sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour isoler le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir "[Configurez les interfaces VLAN](#)".

Configurer la fédération des identités et SSO

Si vous prévoyez d'utiliser la fédération 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 des identités](#)" et "[Configurer l'authentification unique](#)".

Obtenir et configurer des noms de domaine

Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées de serveur de noms de domaine (DNS) mapperont ce FQDN aux adresses IP virtuelles (VIP) du groupe haute disponibilité que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, vous devriez avoir "[Noms de domaine de terminaux S3 configurés](#)". L'utilisation de requêtes de type hébergement virtuel est recommandée.

Examinez les exigences en matière d'équilibreur de charge et de certificat de sécurité

Si vous envisagez d'utiliser l'équilibreur de charge StorageGRID, vous avez examiné les considérations générales relatives à l'équilibrage de la charge. Vous disposez des certificats que vous allez télécharger ou des valeurs dont vous avez besoin pour générer un certificat.

Si vous prévoyez d'utiliser un nœud final externe (tiers) d'équilibreur de charge, vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurez toutes les connexions de fédération de grille

Si vous souhaitez autoriser le locataire S3 à synchroniser les données du compte et à répliquer les objets du compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles, confirmez les points suivants avant de démarrer l'assistant :

- Vous avez "[configurez la connexion de fédération de grille - effectué](#)".
- L'état de la connexion est **connecté**.
- Vous disposez de l'autorisation d'accès racine.

Accédez et complétez l'assistant de configuration S3 dans StorageGRID

L'assistant d'installation de S3 vous permet de configurer StorageGRID pour une utilisation avec une application S3. L'assistant d'installation fournit les valeurs dont l'application a besoin pour accéder à un compartiment StorageGRID et pour enregistrer des objets.

Avant de commencer

- Vous avez le "[Autorisation d'accès racine](#)".
- Vous avez examiné le "[considérations et exigences](#)" pour à l'aide de l'assistant.

Accéder à l'assistant

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
2. Si la bannière **FabricPool and S3 setup wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide  dans la barre d'en-tête du Grid Manager et sélectionnez **FabricPool and S3 setup wizard**.
3. Dans la section application S3 de la page de l'assistant d'installation FabricPool et S3, sélectionnez **configurer maintenant**.

Étape 1 sur 6 : configuration du groupe haute disponibilité

Un groupe haute disponibilité est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données S3 disponibles. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations S3.

Pour plus de détails sur cette tâche, reportez-vous "[Gérez les groupes haute disponibilité](#)" à la section .

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, il n'est pas nécessaire de créer un groupe haute disponibilité. Sélectionnez **Ignorer cette étape** et passez à [Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge](#).
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe haute disponibilité ou utiliser un groupe haute disponibilité existant.

Création du groupe haute disponibilité

- a. Pour créer un nouveau groupe HA, sélectionnez **Create HA group**.
- b. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

- c. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

- d. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP reviennent à l'interface de priorité la plus élevée disponible.

- e. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR ; adresse IPv4 suivie d'une barre oblique et de la longueur de sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple 192.16.0.0/22, .
Adresse IP de la passerelle (facultative)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Create HA group**, puis **Finish** pour revenir à l'assistant d'installation S3.

g. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Utilisez un groupe haute disponibilité existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans le **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir des applications client. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service StorageGRID Load Balancer, qui existe sur tous les nœuds de passerelle et d'administration, ou vous pouvez vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, reportez-vous ["Considérations relatives à l'équilibrage de charge"](#) à la section .

Pour utiliser le service StorageGRID Load Balancer, sélectionnez l'onglet **StorageGRID load balancer**, puis créez ou sélectionnez le nœud final de l'équilibreur de charge que vous souhaitez utiliser. Pour utiliser un équilibreur de charge externe, sélectionnez l'onglet **équilibreur de charge externe** et fournissez des détails sur le système que vous avez déjà configuré.

Créer un point final

Étapes

1. Pour créer un noeud final d'équilibrage de charge, sélectionnez **Créer un noeud final**.
2. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir "Ports internes StorageGRID".
Type de client	Doit être S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

3. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accessible à l'aide d'une 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 final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce nœud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

4. Pour l'étape d'accès locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce nœud final.

5. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
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 d'API S3" pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant d'installation S3.

7. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utilisez le terminal d'équilibrage de charge existant

Étapes

1. Pour utiliser un noeud final existant, sélectionnez son nom dans le **sélectionnez un noeud final d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, renseignez les champs suivants.

Champ	Description
FQDN	Nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Numéro de port que l'application S3 utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

2. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Étape 3 sur 6 : création d'un locataire et d'un compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire dispose de ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités.

Un compartiment est un conteneur utilisé pour stocker les objets d'un locataire et ses métadonnées d'objet. Même si les locataires peuvent disposer de plusieurs compartiments, l'assistant vous aide à créer un locataire et un compartiment de la manière la plus rapide et la plus simple. Si vous avez besoin d'ajouter des compartiments ou de définir des options ultérieurement, vous pouvez utiliser le Gestionnaire de locataires.

Pour plus d'informations sur cette tâche, reportez-vous aux sections "[Créer un compte de locataire](#)" et "[Créer un compartiment S3](#)".

Étapes

1. Entrez un nom pour le compte de locataire.

Les noms de locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.

2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise "[fédération des identités](#)", "[Authentification unique \(SSO\)](#)", ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.

Option	Faites ça
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant " Autorisation d'accès racine " pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant " Autorisation d'accès racine " pour le tenant. 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 tenant sera l'utilisateur root. Si d'autres utilisateurs utilisent ce locataire, "[Utilisez le gestionnaire de locataires](#)" pour configurer les clés et les autorisations.

4. Si vous voulez créer un compartiment pour ce tenant maintenant, sélectionnez **Créer un compartiment pour ce tenant**.



Si le verrouillage d'objet S3 est activé pour la grille, le verrouillage d'objet S3 n'est pas activé pour le compartiment créé à cette étape. Si vous avez besoin d'utiliser un compartiment S3 Object Lock pour cette application S3, ne créez pas de compartiment maintenant. Utilisez plutôt le gestionnaire de locataires "[créer le godet](#)" plus tard.

- a. Entrez le nom du compartiment que l'application S3 utilisera. Par exemple `s3-bucket`, .

Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

- b. Sélectionnez la **région** pour ce compartiment.

Utilisez la région par défaut (`us-east-1`) à moins d'utiliser ILM à l'avenir pour filtrer des objets en fonction de la région du compartiment.

5. Sélectionnez **Créer et continuer**.

étape 4 sur 6 : télécharger les données

Dans l'étape de téléchargement des données, vous pouvez télécharger un ou deux fichiers pour enregistrer les détails de ce que vous venez de configurer.

Étapes

- Si vous avez sélectionné **Créer la clé d'accès S3 de l'utilisateur root automatiquement**, effectuez l'une des opérations suivantes ou les deux :
 - Sélectionnez **Télécharger les clés d'accès** pour télécharger un `.csv` fichier contenant le nom du compte du locataire, l'ID de la clé d'accès et la clé d'accès secrète.
 - Sélectionnez l'icône de copie () pour copier l'ID de 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 noeud final de l'équilibreur de charge, du locataire, du compartiment et de l'utilisateur root.

3. Enregistrez ces informations dans un emplacement sécurisé.



Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les touches ne seront pas disponibles après la fermeture de cette page. Veuillez à enregistrer ces informations dans un emplacement sécurisé car elles peuvent être utilisées pour obtenir des données de votre système StorageGRID.

4. Si vous y êtes invité, cochez la case pour confirmer que vous avez téléchargé ou copié les clés.

5. Sélectionnez **Continuer** pour accéder à la règle ILM et à l'étape de stratégie.

Étape 5 sur 6 : examen de la règle ILM et de la règle ILM pour S3

Les règles de gestion du cycle de vie des informations (ILM) contrôlent le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID. La règle ILM incluse à StorageGRID effectue deux copies répliquées de tous les objets. Cette stratégie est en vigueur jusqu'à ce que vous activiez au moins une nouvelle police.

Étapes

1. Passez en revue les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou compartiment, créez une règle et une nouvelle règle. Voir "[Création d'une règle ILM](#)" et "[Règles ILM](#)".
3. Sélectionnez **J'ai passé en revue ces étapes et je comprends ce que je dois faire**.
4. Cochez la case pour indiquer que vous comprenez ce qu'il faut faire ensuite.
5. Sélectionnez **Continuer** pour accéder à **Résumé**.

Étape 6 sur 6 : passez en revue le résumé

Étapes

1. Passez en revue le résumé.
2. Notez les détails des étapes suivantes, qui décrivent la configuration supplémentaire qui peut être nécessaire avant de vous connecter au client S3. Par exemple, la sélection de **se connecter en tant que root** vous amène au gestionnaire de locataires, où vous pouvez ajouter des utilisateurs de tenant, créer des compartiments supplémentaires et mettre à jour les paramètres de compartiment.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier téléchargé à partir de StorageGRID ou des valeurs obtenues manuellement.

Gérer les groupes de haute disponibilité

Découvrez les groupes de haute disponibilité StorageGRID

Les groupes haute disponibilité proposent des connexions de données extrêmement disponibles pour les clients S3 et des connexions extrêmement disponibles pour Grid Manager et tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité. En cas de défaillance de l'interface active dans le groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail.

Chaque groupe HA permet d'accéder aux services partagés sur les nœuds sélectionnés.

- Les groupes HAUTE DISPONIBILITÉ, tels que les nœuds de passerelle et/ou les nœuds d'administration, assurent des connexions de données extrêmement disponibles pour les clients S3.
- Les groupes HAUTE DISPONIBILITÉ comprenant uniquement des nœuds d'administration fournissent des connexions hautement disponibles au Grid Manager et au tenant Manager.
- Un groupe haute disponibilité qui ne comprend que des appliances de services et des nœuds logiciels VMware peut fournir des connexions hautement disponibles pour "[Locataires S3 avec S3 Select](#)". Les groupes HAUTE DISPONIBILITÉ sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Comment créer un groupe haute disponibilité ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface réseau client (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.



Vous ne pouvez pas ajouter d'interface à un groupe haute disponibilité si son adresse IP est attribuée par DHCP.

2. Vous spécifiez une interface à utiliser comme interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous affectez une à 10 adresses IP virtuelles (VIP) au groupe. Les applications clients peuvent utiliser l'une de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, reportez-vous à la section "[Configurez les groupes haute disponibilité](#)".

Qu'est-ce que l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe haute disponibilité sont ajoutées à l'interface principale, qui est la première interface dans l'ordre prioritaire. Tant que l'interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n'importe quelle adresse VIP pour le groupe. C'est-à-dire, pendant le fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, pendant le fonctionnement normal, toute interface de priorité inférieure du groupe haute disponibilité fait office d'interfaces de « sauvegarde ». Ces interfaces de sauvegarde ne sont utilisées que si l'interface principale (actuellement active) est indisponible.

Afficher l'état actuel du groupe haute disponibilité d'un nœud

Pour voir si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **Nœuds > node**.

Si l'onglet **Présentation** inclut une entrée pour **groupes HA**, le nœud est affecté aux groupes HA répertoriés. La valeur après le nom du groupe est l'état actuel du nœud du groupe HA :

- **Actif** : le groupe HA est actuellement hébergé sur ce nœud.
- **Backup** : le groupe HA n'utilise pas ce nœud, c'est une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service haute disponibilité (keepalived) a été arrêté manuellement.
- **Fault** : le groupe HA ne peut pas être hébergé sur ce nœud en raison d'un ou plusieurs des éléments suivants :

- Le service Load Balancer (ninx-gw) n'est pas exécuté sur le nœud.
- L'interface eth0 ou VIP du nœud est en panne.
- Le nœud ne fonctionne pas.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active du groupe clients Admin et une interface de sauvegarde pour le groupe clients FabricPool.

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 tombe en panne ?

L'interface qui héberge actuellement les adresses VIP est l'interface active. Si le groupe haute disponibilité inclut plusieurs interfaces et que l'interface active tombe en panne, les adresses VIP sont transférées vers la première interface de sauvegarde disponible dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à la prochaine interface de sauvegarde disponible, etc.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée s'éteint.
- Le nœud sur lequel l'interface est configurée perd la connectivité sur tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service haute disponibilité s'arrête.



Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par les services pour le Grid Manager ou le tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes aient peu d'impact et peuvent compter sur des comportements de tentatives normales pour poursuivre le fonctionnement.

Lorsqu'une panne est résolue et qu'une interface de priorité supérieure est à nouveau disponible, les adresses VIP sont automatiquement transférées vers l'interface de priorité la plus élevée disponible.

Comment les groupes HA de StorageGRID assurent une haute disponibilité

Vous pouvez utiliser des groupes haute disponibilité pour fournir des connexions extrêmement disponibles à StorageGRID pour les données d'objet et pour les tâches d'administration.

- Un groupe haute disponibilité peut fournir des connexions administratives hautement disponibles vers le Grid Manager ou le tenant Manager.
- Un groupe haute disponibilité peut fournir des connexions de données extrêmement disponibles pour les clients S3.
- Un groupe haute disponibilité ne contenant qu'une interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe haute disponibilité peut assurer la haute disponibilité uniquement si tous les nœuds du groupe fournissent les mêmes services. Lorsque vous créez un groupe haute disponibilité, ajoutez des interfaces à partir des types de nœuds qui fournissent les services requis.

- **Nœuds d'administration** : incluez le service Load Balancer et activez l'accès au Grid Manager ou au Gestionnaire de locataires.
- **Nœuds de passerelle** : inclure le service Load Balancer.

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès à Grid Manager	• Nœud d'administration principal (primaire) • Nœuds d'administration non primaires Remarque : le nœud d'administration principal doit être l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.
Accès au Gestionnaire de locataires uniquement	• Nœuds d'administration primaires ou non primaires
Accès client S3 – Service d'équilibrage de charge	• Nœuds d'administration • Nœuds de passerelle

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès client S3 pour "S3 Select"	• Appliances de services • Nœuds logiciels VMware Remarque : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Restrictions liées à l'utilisation de groupes haute disponibilité avec Grid Manager ou tenant Manager

En cas de défaillance d'un service Grid Manager ou tenant Manager, le basculement du groupe haute disponibilité n'est pas déclenché.

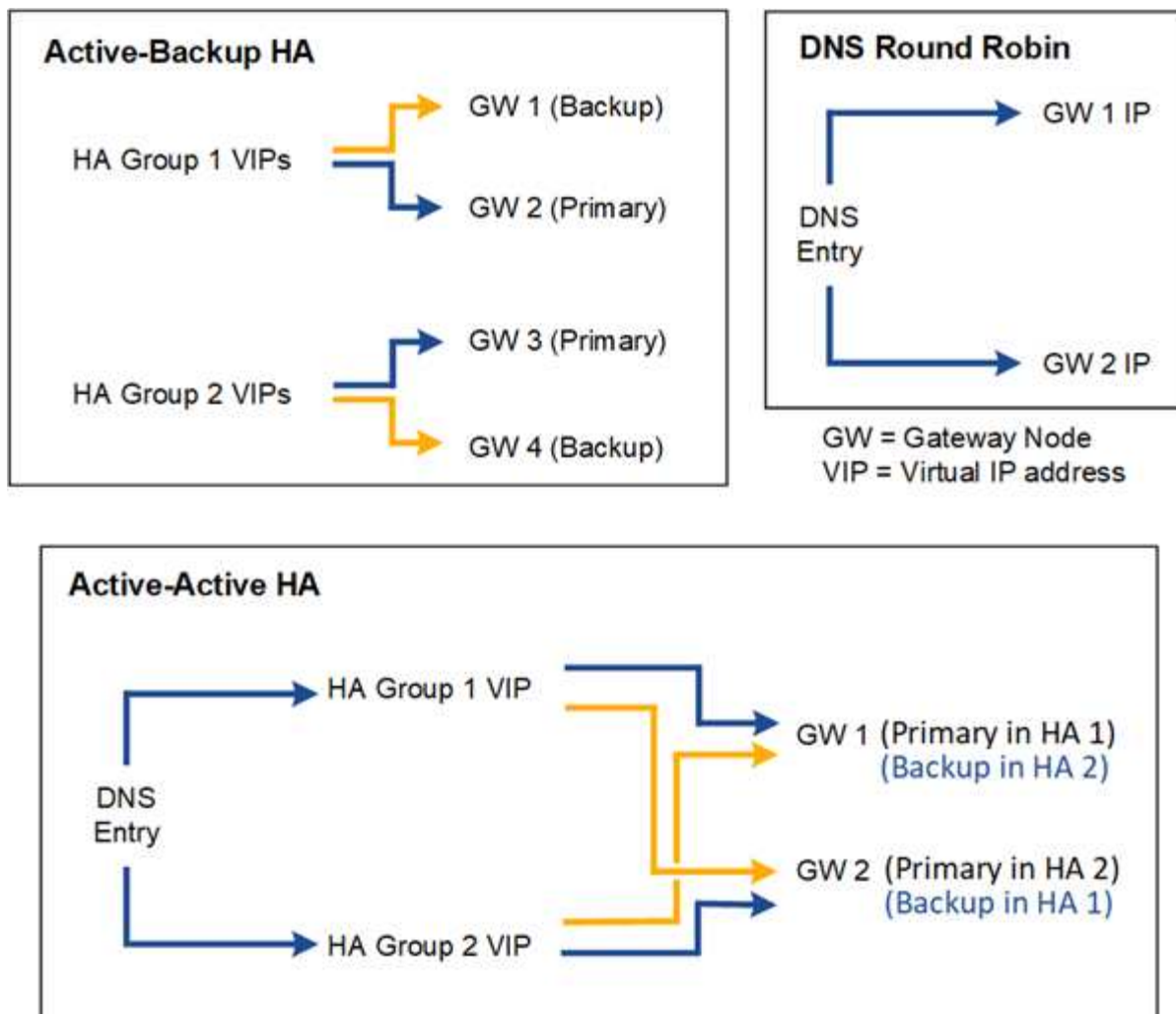
Si vous êtes connecté au Grid Manager ou au tenant Manager lors du basculement, vous êtes déconnecté et vous devez vous reconnecter pour reprendre votre tâche.

Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Pendant le basculement, vous pouvez utiliser le Gestionnaire de grille pour surveiller votre système StorageGRID.

Options de configuration pour les groupes à haute disponibilité StorageGRID

Les schémas suivants présentent des exemples de différentes façons dont vous pouvez configurer des groupes à haute disponibilité (HA). Chaque option comporte des avantages et des inconvénients.

Dans les schémas, le bleu indique l'interface principale du groupe haute disponibilité et la jaune indique l'interface de sauvegarde du groupe haute disponibilité.



Le tableau récapitule les avantages de chaque configuration de haute disponibilité illustrée sur le schéma.

Configuration	Avantages	Inconvénients
Active-Backup HA	- Gérées par StorageGRID sans dépendances externes - Basculement rapide	Un seul nœud d'un groupe haute disponibilité est actif. Au moins un nœud par groupe haute disponibilité sera inactif.
DNS Round Robin	- Un débit global supérieur. - Aucun hôte inactif.	- Basculement lent, qui peut dépendre du comportement des clients. - Nécessite une configuration matérielle en dehors du StorageGRID. - Nécessite une vérification de l'état implémentée par le client.

Configuration	Avantages	Inconvénients
Haute disponibilité actif-actif	• Le trafic est réparti entre plusieurs groupes haute disponibilité. • Débit global élevé qui évolue en même temps que le nombre de groupes HA. • Basculement rapide	• Configuration plus complexe. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.

Configurez des groupes de haute disponibilité dans StorageGRID

Vous pouvez configurer des groupes haute disponibilité pour fournir un accès haute disponibilité aux services sur des nœuds d'administration ou de passerelle.



Un système StorageGRID peut avoir un maximum de 255 groupes HA.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe haute disponibilité, vous avez créé cette interface. Voir ["Configurez les interfaces VLAN"](#).
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud d'un groupe haute disponibilité, vous avez créé l'interface :
 - **Linux (avant l'installation du nœud):** ["Créez des fichiers de configuration de nœud"](#)
 - **Linux (après l'installation du nœud):** ["Ajouter des interfaces de jonction ou d'accès à un nœud"](#)
 - **VMware (après l'installation du nœud):** ["Ajouter des interfaces de jonction ou d'accès à un nœud"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Créez un groupe haute disponibilité

Lorsque vous créez un groupe haute disponibilité, vous sélectionnez une ou plusieurs interfaces et organisez-les par ordre de priorité. Vous affectez ensuite une ou plusieurs adresses VIP au groupe.

Pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe haute disponibilité, une interface doit être configurée pour inclure un nœud de passerelle. Un groupe haute disponibilité ne peut utiliser qu'une interface pour un nœud donné. Toutefois, les autres interfaces du même nœud peuvent être utilisées dans d'autres groupes haute disponibilité.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe haute disponibilité

Étapes

1. Indiquez un nom unique pour le groupe HA.
2. Si vous le souhaitez, entrez une description pour le groupe HA.
3. Sélectionnez **Continuer**.

Ajouter des interfaces au groupe haute disponibilité

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

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



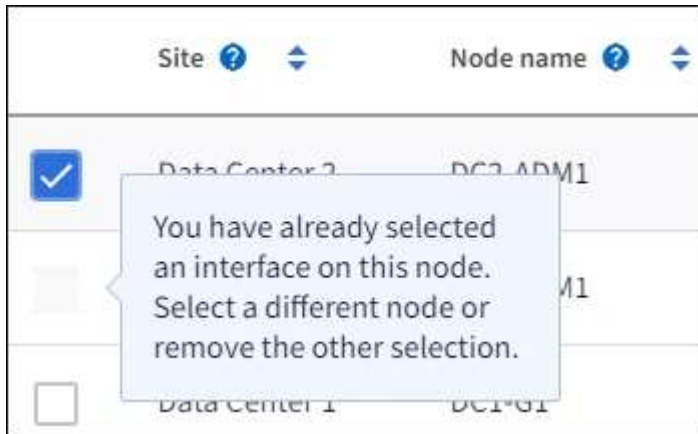
Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes que la nouvelle interface apparaisse dans le tableau.

Consignes de sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une interface pour un nœud.
- Si le groupe HA est destiné à la protection haute disponibilité des services des nœuds d'administration, qui incluent le Grid Manager et le tenant Manager, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si le groupe haute disponibilité est dédié à la protection HA du trafic client S3, sélectionnez interfaces sur les nœuds d'administration, nœuds de passerelle, ou les deux.
- Si vous sélectionnez des interfaces sur différents types de nœuds, une note d'information s'affiche. Il est rappelé que en cas de basculement, les services fournis par le nœud actif précédemment risquent

de ne pas être disponibles sur le nouveau nœud actif. Par exemple, un nœud de passerelle de sauvegarde ne peut pas assurer la protection haute disponibilité des services du nœud d'administration. De même, un nœud d'administration des sauvegardes ne peut pas effectuer toutes les procédures de maintenance que le nœud d'administration principal peut fournir.

- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L'info-bulle fournit plus d'informations.



- Vous ne pouvez pas sélectionner d'interface si sa valeur de sous-réseau ou sa passerelle entre en conflit avec une autre interface sélectionnée.
- Vous ne pouvez pas sélectionner une interface configurée si elle ne possède pas d'adresse IP statique.

2. Sélectionnez **Continuer**.

Déterminez l'ordre de priorité

Si le groupe haute disponibilité comprend plusieurs interfaces, vous pouvez déterminer qui est l'interface principale et quelles sont les interfaces de sauvegarde (basculement). Si l'interface principale échoue, les adresses VIP passent à l'interface de priorité la plus élevée disponible. En cas d'échec de cette interface, les adresses VIP passent à l'interface de priorité supérieure suivante disponible, etc.

Étapes

1. Faites glisser des lignes dans la colonne **ordre de priorité** pour déterminer l'interface principale et les interfaces de sauvegarde.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

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 donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

2. Sélectionnez **Continuer**.

Saisissez les adresses IP

Étapes

1. Dans le champ **Subnet CIDR**, spécifiez le sous-réseau VIP en notation CIDR—une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32).

Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple 192.16.0.0/22, .



Si vous utilisez un préfixe 32 bits, l'adresse réseau VIP sert également d'adresse de passerelle et d'adresse VIP.

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](#)

- Si vous le souhaitez, si des clients d'administration ou de locataire S3 accèdent à ces adresses VIP à partir d'un sous-réseau différent, entrez l'adresse IP **Gateway**. L'adresse de la passerelle doit se trouver dans le sous-réseau VIP.

Les utilisateurs client et admin utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

- Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP et toutes seront actives en même temps sur l'interface active.

Vous devez fournir au moins une adresse IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

- Sélectionnez **Créer groupe HA** et **Terminer**.

Le groupe haute disponibilité est créé et vous pouvez maintenant utiliser les adresses IP virtuelles configurées.

Étapes suivantes

Si vous utilisez ce groupe haute disponibilité pour équilibrer la charge, créez un terminal d'équilibreur de charge afin de déterminer le port et le protocole réseau, et de connecter tous les certificats requis. Voir ["Configurer les terminaux de l'équilibreur de charge"](#).

Modifiez un groupe haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour modifier son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous devrez peut-être modifier un groupe haute disponibilité si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans la procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.

La page groupes haute disponibilité affiche tous les groupes haute disponibilité existants.

2. Cochez la case du groupe haute disponibilité à modifier.
3. Effectuez l'une des opérations suivantes, en fonction de ce que vous souhaitez mettre à jour :
 - Sélectionnez **actions > Modifier l'adresse IP virtuelle** pour ajouter ou supprimer des adresses VIP.
 - Sélectionnez **actions > Modifier le groupe HA** pour mettre à jour le nom ou la description du groupe, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou supprimer des adresses VIP.
4. Si vous avez sélectionné **Modifier l'adresse IP virtuelle** :
 - a. Mettre à jour les adresses IP virtuelles du groupe haute disponibilité.
 - b. Sélectionnez **Enregistrer**.
 - c. Sélectionnez **Terminer**.
5. Si vous avez sélectionné **Modifier le groupe HA** :
 - a. Vous pouvez également mettre à jour le nom ou la description du groupe.
 - b. Vous pouvez également cocher ou décocher les cases pour ajouter ou supprimer des interfaces.



Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal

- c. Vous pouvez également faire glisser des lignes pour modifier l'ordre de priorité de l'interface principale et des interfaces de sauvegarde de ce groupe haute disponibilité.
- d. Si vous le souhaitez, mettez à jour les adresses IP virtuelles.
- e. Sélectionnez **Enregistrer**, puis **Terminer**.

Supprimer un groupe haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes haute disponibilité (HA) à la fois.



Vous ne pouvez pas supprimer un groupe haute disponibilité s'il est lié à un terminal d'équilibrage de charge. Pour supprimer un groupe haute disponibilité, vous devez le supprimer de tous les terminaux d'équilibrage de charge qui l'utilisent.

Pour éviter toute interruption de service, mettez à jour toutes les applications client S3 affectées avant de supprimer un groupe haute disponibilité. Mettre à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe haute disponibilité ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Consultez la colonne **Load Balancer Endpoints** pour chaque groupe HA que vous souhaitez supprimer. Si des terminaux d'équilibrage de charge sont répertoriés :

- a. Accédez à **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Cochez la case du point final.
 - c. Sélectionnez **actions > Modifier le mode de liaison du point final**.
 - d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
 - e. Sélectionnez **Enregistrer les modifications**.
3. Si aucun point final de l'équilibreur de charge n'est répertorié, cochez la case de chaque groupe haute disponibilité à supprimer.
 4. Sélectionnez **actions > Supprimer groupe HA**.
 5. Vérifiez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

Tous les groupes HA sélectionnés sont supprimés. Une bannière de réussite verte apparaît sur la page groupes de haute disponibilité.

Gérer l'équilibrage des charges

Découvrez l'équilibrage de charge StorageGRID

L'équilibrage des charges vous permet de gérer les workloads d'ingestion et de récupération à partir des clients S3.

Qu'est-ce que l'équilibrage de la charge ?

Lorsqu'une application client enregistre ou récupère les données d'un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service StorageGRID Load Balancer est installé sur tous les nœuds d'administration et sur tous les nœuds de passerelle. Il assure l'équilibrage de la charge de couche 7. Il effectue la résiliation du protocole TLS (transport Layer Security) des requêtes du client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage.

Le service Load Balancer de chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure.



Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de charge recommandé, vous souhaitez peut-être intégrer un équilibreur de charge tiers à la place. Pour plus d'informations, contactez votre représentant commercial NetApp ou consultez ["Utilisez des équilibreurs de charge tiers avec StorageGRID"](#).

De combien de nœuds d'équilibrage de charge ai-je besoin ?

Dans le cadre des meilleures pratiques générales, chaque site de votre système StorageGRID doit inclure au moins deux nœuds avec le service Load Balancer. Par exemple, un site peut inclure deux nœuds de passerelle ou un nœud d'administration et un nœud de passerelle. 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.

Qu'est-ce qu'un terminal d'équilibrage de charge ?

Un noeud final d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) utilisés par les demandes d'applications clientes entrantes et sortantes pour accéder aux noeuds qui contiennent le service d'équilibrage de charge. Le noeud final 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, utilisez le gestionnaire de grille ou suivez les assistants de configuration S3 et FabricPool :

- ["Configurer les terminaux de l'équilibreur de charge"](#)
- ["Utilisez l'assistant d'installation S3"](#)
- ["Utilisez l'assistant de configuration FabricPool"](#)

Considérations relatives à la mise en cache de l'équilibreur de charge

La mise en cache améliore considérablement les performances lorsqu'une charge de travail fonctionne sur un sous-ensemble de données et accède aux objets plusieurs fois. De plus, la mise en cache fournit un accès à distance au stockage d'objets sans déploiement de grille complet. La mise en cache de l'équilibreur de charge est disponible uniquement pour les nœuds de passerelle.

Lorsque vous créez des points de terminaison d'équilibrage de charge :

- Activez la mise en cache uniquement pour les charges de travail pouvant être mises en cache. Les charges de travail qui accèdent aux données non mises en cache plus souvent qu'aux données mises en cache auront des performances inférieures à celles obtenues si elles n'avaient pas été traitées par le cache. Dans certains cas, les charges de travail avec des taux d'écrasement et d'éviction élevés peuvent également dépasser l'endurance d'écriture garantie du lecteur.
- Envisagez d'ajouter des points de terminaison ou des nœuds supplémentaires pour la mise en cache des charges de travail individuelles qui sont de bons candidats pour la mise en cache.
- Utilisez des points de terminaison distincts pour les charges de travail pouvant être mises en cache et non mises en cache. Cette séparation garantit que les mécanismes de mise en cache sont appliqués de manière appropriée et n'interfèrent pas avec le traitement des données non cachables.
- Évaluez une charge de travail potentiellement cachable en la dirigeant vers le point de terminaison activé pour le cache. Surveillez et vérifiez le taux de réussite du cache pour déterminer l'adéquation de la charge de travail à la mise en cache. Cette évaluation permet d'optimiser les performances et de garantir une utilisation efficace des ressources du cache.
- ["Examiner les journaux d'audit"](#) pour déterminer si une charge de travail existante serait un bon candidat pour la mise en cache. Pour une période donnée, déterminez quel pourcentage de GET concerne des objets uniques. Pour être adaptée à la mise en cache, cette valeur doit être inférieure à 50 %.

Exemples de charges de travail qui pourraient être de bons candidats à la mise en cache

- Lacs de données
- Calcul haute performance (HPC)
- Formation IA/ML
- Réseaux de distribution de contenu (CDN)
- Gestion des ressources multimédias
- Production vidéo



- Plusieurs versions d'objets peuvent être mises en cache.
- Les opérations de lecture de plage sont prises en charge.

Exemples de charges de travail qui ne sont pas de bons candidats à la mise en cache

- Piscine en tissu
- Applications de sauvegarde
- hiérarchisation du stockage



Si un contenu à servir par le cache nécessite un chiffrement au repos, "[activer le chiffrement du nœud ou du lecteur](#)" sur le nœud de cache.

Types d'objets et de requêtes qui ne seront pas mis en cache

- Le `response-content-encoding` paramètre de requête
- Le `partNumber` paramètre de requête
- En-têtes conditionnels
 - `If-Match`
 - `If-Modified-Since`
 - `If-None-Match`
 - `If-Unmodified-Since`
- Les requêtes qui ont été chiffrées au repos avec l'un des éléments suivants :
 - SSE (chiffrement côté serveur avec clés gérées par StorageGRID)
 - SSE-C (chiffrement côté serveur avec clés fournies par le client)
 - Chiffrement des objets stockés

Toutes les demandes qui ne sont pas mises en cache sont transmises à un LDR en amont comme si le cache n'était pas activé.

Informations associées

- "[Résoudre les problèmes de mise en cache de l'équilibreur de charge](#)"
- Pour plus d'informations sur la mise en cache de l'équilibreur de charge, contactez le support technique.

Considérations relatives au port

Par défaut, le port d'un nœud final d'équilibrage de charge est 10433 pour le premier nœud final que vous créez, mais vous pouvez spécifier tout port externe inutilisé compris entre 1 et 65535. Si vous utilisez le port 80 ou 443, le nœud final utilisera le service Load Balancer sur les nœuds passerelle uniquement. Ces ports sont réservés sur des nœuds d'administration. Si vous utilisez le même port pour plusieurs nœuds finaux, vous devez spécifier un mode de liaison différent pour chaque nœud final.

Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir "[Ports internes StorageGRID](#)".

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le chiffrement TLS (transport Layer Security). La connexion à StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée, en particulier dans les environnements de production. Lorsque vous sélectionnez le protocole réseau pour le noeud final de l'équilibreur de charge StorageGRID, vous devez sélectionner **HTTPS**.

Considérations relatives aux certificats de terminaux d'équilibrage de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le noeud final de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Lorsque vous créez le terminal de l'équilibreur de charge, vous pouvez utiliser l'une de ces trois options :

- **Télécharger un certificat signé (recommandé).** Ce certificat peut être signé par une autorité de certification publique ou privée. Il est recommandé d'utiliser un certificat de serveur d'autorité de certification de confiance publique pour sécuriser la connexion. Contrairement aux certificats générés, les certificats signés par une autorité de certification peuvent être permutés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

Vous devez obtenir les fichiers suivants avant de créer le noeud final de l'équilibreur de charge :

- Le fichier de certificat de serveur personnalisé.
- Le fichier de clé privée du certificat de serveur personnalisé.
- Éventuellement, un paquet CA des certificats de chaque autorité de certification intermédiaire émettrice.
- **Générer un certificat auto-signé.**
- **Utilisez le certificat StorageGRID S3 global.** Vous devez télécharger ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le noeud final de l'équilibreur de charge. Voir "[Configurer les certificats d'API S3](#)".

Quelles valeurs ai-je besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP utilisés par les applications client S3 pour accéder au terminal.

L'entrée **Subject DN** (Distinguished Name) du certificat doit inclure le nom de domaine complet que l'application client utilisera pour StorageGRID. Par exemple :

```
Subject DN:  
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Si nécessaire, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et nœuds de passerelle exécutant le service Load Balancer. Par exemple, *.storagegrid.example.com utilise le caractère générique * pour représenter adm1.storagegrid.example.com et gn1.storagegrid.example.com.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, le certificat doit également inclure une entrée **Nom alternatif** pour chaque "[Nom du domaine du terminal S3](#)" que vous avez configuré, y compris tout nom générique. Par exemple :

Alternative Name: DNS:*.s3.storagegrid.example.com



Si vous utilisez des caractères génériques pour les noms de domaine, consultez le "[Consignes de renforcement des certificats de serveur](#)".

Vous devez également définir une entrée DNS pour chaque nom du certificat de sécurité.

Comment gérer les certificats arrivant à expiration ?



Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application risque de perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez les bonnes pratiques suivantes :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que le **expiration du certificat de noeud final de l'équilibreur de charge** et le **expiration du certificat de serveur global pour les alertes de l'API S3**.
- Synchronisez toujours les versions du certificat des applications StorageGRID et S3. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez remplacer les certificats bientôt expirés sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans l'application S3 avant que le certificat existant n'expire.

Considérations relatives au mode de liaison

Le mode de liaison vous permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un noeud final de l'équilibreur de charge. Si un noeud final utilise un mode de liaison, les applications clientes peuvent uniquement accéder au noeud final si elles utilisent une adresse IP autorisée ou son nom de domaine complet (FQDN) correspondant. Les applications clientes utilisant une autre adresse IP ou un autre nom de domaine complet ne peuvent pas accéder au point final.

Vous pouvez spécifier l'un des modes de reliure suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au noeud final en utilisant l'adresse IP de n'importe quel noeud de passerelle ou noeud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez ce paramètre, sauf si vous avez besoin de restreindre l'accessibilité d'un noeud final.
- **Adresses IP virtuelles des groupes HA**. Les applications client doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité.
- **Interfaces de nœud**. Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées.
- **Type de nœud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle.

Considérations relatives à l'accès des locataires

L'accès aux locataires est une fonction de sécurité facultative qui vous permet de contrôler quels comptes de locataires StorageGRID peuvent utiliser un terminal d'équilibrage des charges pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un noeud final (par défaut), ou vous pouvez spécifier une liste des locataires autorisés ou bloqués pour chaque noeud final.

Vous pouvez utiliser cette fonction pour améliorer l'isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonction pour vous assurer que les matériaux les plus secrets ou les matériaux hautement classés appartenant à un locataire restent complètement inaccessibles aux autres locataires.



Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la demande du client, si aucune clé d'accès n'est fournie dans le cadre de la demande (par exemple avec un accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès aux locataires

Pour comprendre le fonctionnement de cette fonction de sécurité, prenez l'exemple suivant :

1. Vous avez créé deux terminaux d'équilibrage de charge, comme suit :
 - **Noeud final public** : utilise le port 10443 et permet l'accès à tous les locataires.
 - **Point final Top secret** : utilise le port 10444 et permet l'accès au locataire **Top secret** uniquement. Tous les autres locataires ne peuvent pas accéder à ce noeud final.
2. Le `top-secret.pdf` est dans un seau appartenant au locataire **Top secret**.

Pour accéder au `top-secret.pdf`, un utilisateur du locataire **Top secret** peut émettre une demande GET à `https://w.x.y.z:10444/top-secret.pdf`. Comme ce locataire est autorisé à utiliser le noeud final 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire envoie la même requête à la même URL, il reçoit un message accès refusé immédiat. L'accès est refusé même si les informations d'identification et la signature sont valides.

Disponibilité du processeur

Le service Load Balancer sur chaque nœud d'administration et de passerelle fonctionne de manière indépendante lors du transfert du trafic S3 vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure. Les informations de charge de l'UC du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids de base minimale, même si un nœud indique une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge StorageGRID

Les terminaux d'équilibrage de la 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 noeuds finaux pour accéder au Gestionnaire de grille, au Gestionnaire de

locataires, ou aux deux.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Vous avez examiné le ["considérations relatives à l'équilibrage de charge"](#).
- Si vous avez précédemment remappé un port que vous prévoyez d'utiliser pour le noeud final de l'équilibreur de charge, vous avez ["retirez le schéma de câblage des ports - effectué"](#).
- Vous avez créé tous les groupes à haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HAUTE DISPONIBILITÉ sont recommandés, mais pas obligatoires. Voir ["Gérez les groupes haute disponibilité"](#).
- Si le noeud final de l'équilibreur de charge sera utilisé par ["Locataires S3 pour S3 Select"](#), il ne doit pas utiliser les adresses IP ou les FQDN des nœuds sans système d'exploitation. Seules les appliances de services et les nœuds logiciels basés sur VMware sont autorisés pour les terminaux d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir ["Configurez les interfaces VLAN"](#).
- Si vous créez un noeud final HTTPS (recommandé), vous disposez des informations relatives au certificat de serveur.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

- Pour télécharger un certificat, vous avez besoin du certificat de serveur, de la clé privée de certificat et, éventuellement, d'un bundle CA.
- Pour générer un certificat, vous devez disposer de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au terminal. Vous devez également connaître le sujet (Nom unique).
- Si vous souhaitez utiliser le certificat d'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 d'API S3"](#).

Créer un noeud final d'équilibreur 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, sélectionnez l'onglet **Client S3**.
3. Pour créer un noeud final permettant d'accéder au Gestionnaire de grille, au Gestionnaire de locataires ou aux deux, sélectionnez l'onglet **interface de gestion**.
4. Sélectionnez **Créer**.

Saisissez les détails du point final

Étapes

1. Sélectionnez les instructions appropriées pour entrer les détails du type de point final que vous souhaitez créer.

Client S3

Champ	Description
Nom	Nom descriptif du noeud final, qui apparaîtra dans le tableau sur la page noeuds finaux de l'équilibreur de charge.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé de 1 à 65535. Si vous entrez 80 ou 8443, le noeud final est configuré uniquement sur les noeuds passerelle, sauf si vous avez libéré le port 8443. Vous pouvez ensuite utiliser le port 8443 en tant que terminal S3 et le port sera configuré à la fois sur les nœuds de passerelle et d'administration. Si vous configurez des points de terminaison d'équilibrage de charge pour un "espace de noms global", utilisez le même port pour chaque point de terminaison.
Type de client	Doit être S3 .
Protocole réseau	Protocole réseau utilisé par les clients lors de la connexion à ce noeud final. • Sélectionnez HTTPS pour la communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le noeud final. • Sélectionnez HTTP pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille autre que la production.
Activer la mise en cache	Activer ou désactiver "mise en cache sur les nœuds de passerelle" pour ce point de terminaison d'équilibrage de charge. Si des problèmes surviennent avec la mise en cache, reportez-vous à "Résoudre les problèmes de mise en cache de l'équilibreur de charge".

Interface de gestion

Champ	Description
Nom	Nom descriptif du noeud final, qui apparaîtra dans le tableau sur la page noeuds finaux de l'équilibreur de charge.

Champ	Description
Port	Port StorageGRID que vous souhaitez utiliser pour accéder au Gestionnaire de grille, au Gestionnaire de locataires ou aux deux. • Gestionnaire de grille : 8443 • Gestionnaire de locataires : 9443 • Gestionnaire de grille et gestionnaire de locataire : 443 Remarque : vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio de l'interface StorageGRID à laquelle vous allez accéder à l'aide de ce noeud final.
Réseau client non fiable	Sélectionnez Oui si ce noeud final 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 qu'un port pour qu'il soit ouvert ou fermé aux réseaux clients non approuvés lorsque vous créez le noeud final de l'équilibreur de charge.

1. Sélectionnez **Continuer**.

Sélectionnez un mode de reliure

Étapes

1. Sélectionnez un mode de liaison pour le noeud final afin de contrôler la façon dont le noeud final 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 noeuds finaux clients ou les noeuds finaux de l'interface de gestion. Tous les modes pour les deux types de point final sont répertoriés ici.

Mode	Description
Global (par défaut pour les noeuds finaux clients)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global sauf si vous devez restreindre l'accessibilité de ce noeud final.

Mode	Description
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce nœud final.
Type de nœud (terminaux client uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.
Tous les nœuds d'administration (valeur par défaut pour les terminaux de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration pour accéder à ce point final.

Si plusieurs nœuds finaux utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel nœud final utiliser : **adresses IP virtuelles des groupes HA > interfaces de nœud > Type de nœud > Global**.

Si vous créez des terminaux d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **IP virtuelles de groupes HA**, sélectionnez un ou plusieurs groupes HA.

Si vous créez des terminaux d'interface de gestion, sélectionnez les VIP associés uniquement aux nœuds d'administration.

3. Si vous avez sélectionné **Node interfaces**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce nœud final.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit nœuds Admin, qui comprend à la fois le nœud Admin principal et tous les nœuds Admin non primaires, soit nœuds Gateway.

Contrôle de l'accès des locataires



Un nœud final de l'interface de gestion ne peut contrôler l'accès des locataires que lorsque le nœud final possède le [Type d'interface du gestionnaire de locataires](#).

Étapes

1. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte de locataire. Après avoir ajouté des comptes de locataire, vous pouvez modifier le terminal de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

- Si vous créez un noeud final **HTTP**, vous n'avez pas besoin de joindre un certificat. Sélectionnez **Créer** pour ajouter le nouveau noeud final de l'équilibreur de charge. Ensuite, passez à [Une fois que vous avez terminé](#). Sinon, sélectionnez **Continuer** pour joindre le certificat.

Joindre un certificat

Étapes

- Si vous créez un noeud final **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au noeud final.

Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur un nœud d'administration ou des 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 avez les valeurs nécessaires pour générer un certificat personnalisé.
- **Utiliser le certificat StorageGRID S3.** Sélectionnez cette option si vous souhaitez utiliser le certificat d'API S3 global, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

Vous ne pouvez sélectionner cette option que si vous avez remplacé le certificat d'API S3 par défaut, signé par l'autorité de certification de la grille, par un certificat personnalisé signé par une autorité de certification externe. Voir ["Configurer les certificats d'API S3"](#).

- **Utiliser le certificat d'interface de gestion.** Sélectionnez cette option si vous souhaitez utiliser le certificat de l'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** : fichier de certificat de serveur personnalisé dans le codage PEM.
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (.key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Créer**. + le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le terminal.

Générez un certificat

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).

Champ	Description
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Créer**.

Le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce terminal.

Une fois que vous avez terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que le DNS inclut un enregistrement pour associer le nom de domaine complet (FQDN) StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

L'adresse IP que vous entrez dans l'enregistrement DNS dépend de l'utilisation ou non d'un groupe HA de nœuds d'équilibrage de la charge :

- Si vous avez configuré un groupe haute disponibilité, les clients se connectent aux adresses IP virtuelles de ce groupe haute disponibilité.
- Si vous n'utilisez pas de groupe haute disponibilité, les clients se connectent au service StorageGRID Load Balancer à l'aide de l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point final requis, y compris les noms de caractères génériques.

2. Fournir aux clients S3 les informations nécessaires pour se connecter au terminal :

- Numéro de port
- Nom de domaine ou adresse IP complet
- Tous les détails de certificat requis

Afficher et modifier les points finaux de l'équilibreur de charge

Vous pouvez afficher les détails des noeuds finaux existants de l'équilibreur de charge, y compris les métadonnées de certificat d'un noeud final sécurisé. Vous pouvez modifier certains paramètres pour un point final.

- Pour afficher les informations de base de tous les noeuds finaux de l'équilibreur de charge, consultez les tableaux de la page noeuds finaux de l'équilibreur de charge.
- Pour afficher tous les détails sur un noeud final spécifique, y compris les métadonnées du certificat, sélectionnez le nom du noeud final dans le tableau. Les informations affichées varient en fonction du type de noeud final 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 noeud final, utilisez le menu **actions** de la page noeuds finaux du répartiteur de charge.



Si vous perdez l'accès à Grid Manager lors de la modification du port d'un noeud final d'interface de gestion, mettez à jour l'URL et le port pour rétablir l'accès.



Après avoir modifié un noeud final, vous devrez peut-être attendre jusqu'à 15 minutes que vos modifications soient appliquées à tous les noeuds.

Tâche	Menu actions	Page de détails
Modifier le nom du point final	a. Cochez la case du point final. b. Sélectionnez actions > Modifier le nom du point final. c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer.
Modifier le port du point final	a. Cochez la case du point final. b. Sélectionnez actions > Modifier le port de point final c. Entrez un numéro de port valide. d. Sélectionnez Enregistrer.	n/a
Modifier le mode de liaison du point final	a. Cochez la case du point final. b. Sélectionnez actions > Modifier le mode de liaison du point final. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez Modifier le mode de liaison. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez Enregistrer les modifications.
Modifier le certificat de point final	a. Cochez la case du point final. b. Sélectionnez actions > Modifier le certificat de point final. c. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, si nécessaire. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet certificat. c. Sélectionnez Modifier le certificat. d. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, si nécessaire. e. Sélectionnez Enregistrer les modifications.

Tâche	Menu actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case du point final. b. Sélectionnez actions > Modifier l'accès locataire . c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet tenant Access . c. Sélectionnez Modifier l'accès locataire . d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. e. Sélectionnez Enregistrer les modifications .

Supprimez les points finaux de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs noeuds finaux à l'aide du menu **actions**, ou vous pouvez supprimer un seul noeud final de la page de détails.



Pour éviter toute interruption de service, mettez à jour toutes les applications client S3 affectées avant de supprimer un terminal d'équilibrage de la charge. Mettez à jour chaque client pour vous connecter à l'aide d'un port attribué à un autre noeud final de l'équilibreur de charge. Assurez-vous également de mettre à jour les informations de certificat requises.



Si vous perdez l'accès à Grid Manager lors de la suppression d'un noeud final d'interface de gestion, mettez l'URL à jour.

- Pour supprimer un ou plusieurs noeuds finaux :
 - Sur la page équilibreur de charge, cochez la case correspondant à chaque noeud final à supprimer.
 - Sélectionnez **actions > Supprimer**.
 - Sélectionnez **OK**.
- Pour supprimer un noeud final de la page de détails :
 - Dans la page équilibreur de charge, sélectionnez le nom du noeud final.
 - Sélectionnez **Supprimer** sur la page de détails.
 - Sélectionnez **OK**.

Configurez les noms de domaine des points de terminaison S3 dans StorageGRID

Pour prendre en charge les requêtes de type hébergement virtuel S3, vous devez utiliser le gestionnaire Grid pour configurer la liste des noms de domaine de terminaux S3 auxquels les clients S3 se connectent.



L'utilisation d'une adresse IP pour un nom de domaine de noeud final n'est pas prise en charge. Les versions ultérieures empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez confirmé qu'une mise à niveau de la grille n'est pas en cours.



N'apportez aucune modification à la configuration du nom de domaine lorsqu'une mise à niveau de grille est en cours.

Description de la tâche

Pour permettre aux clients d'utiliser les noms de domaine de terminaux S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Assurez-vous que le ["Certificat utilisé par le client pour les connexions HTTPS à StorageGRID"](#) est signé pour tous les noms de domaine requis par le client.

Par exemple, si le noeud final est `s3.company.com`, vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` noeud final et le caractère générique Subject alternative Name (SAN): `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et assurez-vous que les enregistrements référencent tous les noms de domaine de point final S3 requis, y compris les noms génériques.



Les clients peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou en se connectant à l'adresse IP virtuelle d'un groupe haute disponibilité. Vous devez comprendre comment les applications client se connectent à la grille pour inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) au grid peuvent utiliser l'un des certificats suivants :

- Les clients qui se connectent à un noeud final d'équilibreur de charge peuvent utiliser un certificat personnalisé pour ce noeud final. Chaque terminal d'équilibrage de la charge peut être configuré de manière à reconnaître différents noms de domaine de terminaux S3.
- Les clients qui se connectent à un terminal d'équilibrage de charge ou directement à un nœud de stockage peuvent personnaliser le certificat d'API S3 global pour inclure tous les noms de domaine de terminaux S3 requis.



Si vous n'ajoutez pas de noms de domaine de terminaux S3 et que la liste est vide, la prise en charge des demandes de type hébergement virtuel S3 est désactivée.

Ajoutez un nom de domaine de terminal S3

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine de point de terminaison S3**.
2. Entrez le nom de domaine dans le champ **Nom de domaine 1**. Sélectionnez **Ajouter un autre nom de domaine** pour ajouter d'autres noms de domaine.

3. Sélectionnez **Enregistrer**.
4. Assurez-vous que les certificats de serveur utilisés par les clients correspondent aux noms de domaine de noeud final S3 requis.
 - Si les clients se connectent à un noeud final d'équilibreur de charge qui utilise son propre certificat, "[mettez à jour le certificat associé au noeud final](#)".
 - Si les clients se connectent à un terminal d'équilibrage de charge qui utilise le certificat d'API S3 global ou directement aux nœuds de stockage, "[Mettez à jour le certificat d'API S3 global](#)".
5. Ajoutez les enregistrements DNS requis pour vous assurer que les demandes de nom de domaine de point final peuvent être résolues.

Résultat

Maintenant, lorsque les clients utilisent le noeud final *bucket.s3.company.com*, le serveur DNS se résout sur le noeud final correct et le certificat authentifie le noeud final comme prévu.

Renommer un nom de domaine de terminal S3

Si vous modifiez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échouent.

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine de point de terminaison S3**.
2. Sélectionnez le champ de nom de domaine que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimez un nom de domaine de terminal S3

Si vous supprimez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine de point de terminaison S3**.
2. Sélectionnez l'icône de suppression  à côté du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations associées

- "[UTILISEZ L'API REST S3](#)"
- "[Afficher les adresses IP](#)"
- "[Configurez les groupes haute disponibilité](#)"

Adresses IP et ports pour les connexions client StorageGRID

Pour stocker ou récupérer des objets, les applications client S3 se connectent au service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service LDR (local distribution Router), qui est inclus sur tous les nœuds de stockage.

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud grid et le

numéro de port du service sur ce nœud. Vous pouvez également créer des groupes haute disponibilité de nœuds d'équilibrage de la charge pour fournir des connexions haute disponibilité utilisant des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un nom de domaine complet (FQDN) au lieu d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Ce tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Si vous avez déjà créé des terminaux d'équilibrage de charge et des groupes haute disponibilité (HA), reportez-vous à la section [Où trouver les adresses IP](#) pour localiser ces valeurs dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	Port attribué au nœud final de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au nœud final de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	Port attribué au nœud final 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 client au point de terminaison Load Balancer d'un groupe haute disponibilité de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

```
https://VIP-of-HA-group:LB-endpoint-port
```

Par exemple, si l'adresse IP virtuelle du groupe haute disponibilité est 192.0.2.5 et que le numéro de port du terminal de l'équilibreur de charge est 10443, une application peut utiliser l'URL suivante pour se connecter à StorageGRID :

```
https://192.0.2.5:10443
```

Où trouver les adresses IP

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Pour trouver l'adresse IP d'un nœud de grille :
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.

- c. Sélectionnez l'onglet **Aperçu**.
- d. Dans la section informations sur le nœud, notez les adresses IP du nœud.
- e. Sélectionnez **Afficher plus** pour afficher les adresses IPv6 et les mappages d'interface.

Vous pouvez établir des connexions entre les applications client et n'importe quelle adresse IP de la liste :

- **Eth0**: réseau de grille
- **Eth1**: réseau d'administration (facultatif)
- **Eth2**: réseau client (facultatif)



Si vous affichez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe haute disponibilité, l'adresse IP virtuelle du groupe haute disponibilité est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe haute disponibilité :
 - a. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
 - b. Dans le tableau, noter l'adresse IP virtuelle du groupe haute disponibilité.
4. Pour trouver le numéro de port d'un nœud final Load Balancer :
 - a. Sélectionnez **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Notez le numéro de port du nœud final que vous souhaitez utiliser.



Si le numéro de port est 80 ou 443, le nœud final 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 sur les nœuds d'administration.

- c. Sélectionnez le nom du nœud final dans la table.
- d. Vérifiez que le **Type de client** (S3) correspond à l'application cliente qui utilisera le nœud final.

Gestion des réseaux et des connexions

Configurer les paramètres réseau de StorageGRID

Vous pouvez configurer différents paramètres réseau à partir du Gestionnaire de grille pour affiner le fonctionnement de votre système StorageGRID.

Configurez les interfaces VLAN

Vous pouvez "[Créer des interfaces VLAN \(Virtual LAN\)](#)" isoler et partitionner le trafic pour assurer la sécurité, la flexibilité et les performances. Chaque interface VLAN est associée à une ou plusieurs interfaces parents sur les nœuds d'administration et les nœuds de passerelle. Vous pouvez utiliser des interfaces VLAN dans des groupes haute disponibilité et dans des terminaux d'équilibrage de charge pour isoler le trafic client ou administratif par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser "[politiques de classification du trafic](#)" pour identifier et gérer différents types de trafic

réseau, notamment le trafic lié à des compartiments, des locataires, des sous-réseaux clients ou des terminaux d'équilibrage de charge spécifiques. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Instructions pour les réseaux StorageGRID

Vous pouvez utiliser le Gestionnaire de grille pour configurer et gérer les réseaux et les connexions StorageGRID.

Reportez-vous à la section "[Configurer les connexions client S3](#)" pour savoir comment connecter les clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur la topologie réseau, reportez-vous à la section "[Instructions de mise en réseau](#)".

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour l'ensemble du trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux.

Réseau d'administration

Facultatif. Le réseau d'administration est généralement utilisé pour l'administration et la maintenance du système. Il peut également être utilisé pour l'accès au protocole client. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir un accès aux applications client S3, de sorte que le réseau Grid peut être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Directives

- Chaque nœud StorageGRID requiert une interface réseau, une adresse IP, un masque de sous-réseau et une passerelle dédiés pour chaque réseau auquel il est attribué.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une passerelle unique, par réseau et par nœud grid est prise en charge et doit être sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe dans la passerelle, si nécessaire.
- Sur chaque nœud, chaque réseau est mappé à une interface réseau spécifique.

Le réseau	Nom de l'interface
Grille	eth0
Administrateur (en option)	eth1

Le réseau	Nom de l'interface
Client (facultatif)	eth2

- Si le nœud est connecté à une appliance StorageGRID, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, reportez-vous aux instructions d'installation de votre appareil.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client n'est opérationnel qu'après que le nœud de la grille ait rejoint la grille
- Le réseau Admin peut être configuré pendant le déploiement du nœud grid pour permettre l'accès à l'interface utilisateur d'installation avant que la grille soit entièrement installée.

Interfaces en option

Vous pouvez également ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pouvez ajouter une interface de jonction à un nœud Admin ou Gateway, de sorte que vous pouvez utiliser ["Interfaces VLAN"](#) pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser dans un ["Groupe haute disponibilité \(HA\)"](#).

Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :

- **VMware (après l'installation du nœud) :** ["VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"](#)
 - **Linux (avant l'installation du nœud):** ["Créez des fichiers de configuration de nœud"](#)
 - **Linux (après l'installation du nœud):** ["Ajouter des interfaces de jonction ou d'accès à un nœud"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#).

Afficher les adresses IP dans StorageGRID

Vous pouvez afficher l'adresse IP de chaque nœud grid dans votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud de grille sur la ligne de commande et effectuer diverses procédures de maintenance.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Pour plus d'informations sur la modification des adresses IP, reportez-vous à ["Configurez les adresses IP"](#) la section .

Étapes

1. Sélectionnez **Nœuds > nœud de grille > Aperçu**.
2. Sélectionnez **Afficher plus** à droite du titre des adresses IP.

Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.

[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.			

Configure the VLAN interfaces in StorageGRID

Créez des interfaces LAN virtuelles (VLAN) sur les nœuds d'administration et les nœuds de passerelle et utilisez-les 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. Les nœuds sélectionnés dans le groupe HA peuvent utiliser les interfaces VLAN pour partager jusqu'à 10 adresses IP virtuelles, de sorte que si un nœud tombe en panne, un autre nœud prend en charge le trafic vers et depuis les adresses IP virtuelles.

Considerations relatives aux interfaces VLAN

- Vous créez une interface VLAN en entrant un ID VLAN et en choisissant une interface parent sur un ou

plusieurs nœuds.

- Une interface parent doit être configurée comme une interface de ligne réseau au niveau du commutateur.
- Une interface parent peut être la Grid Network (eth0), le réseau client (eth2) ou une interface de ligne de jonction supplémentaire pour la VM ou l'hôte bare-Metal (par exemple, en256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parent pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface réseau Grid et l'interface réseau client sur le même nœud passerelle que l'interface parent pour le même VLAN.
- Si l'interface VLAN est destinée au trafic du nœud d'administration, qui inclut le trafic lié au Grid Manager et au Gestionnaire de locataires, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si l'interface VLAN est destinée au trafic client S3, sélectionnez les interfaces sur les nœuds d'administration ou les nœuds de passerelle.
- Si vous avez besoin d'ajouter des interfaces de jonction, consultez les informations suivantes :
 - **VMware (après l'installation du nœud)** : ["VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"](#)
 - **Linux (avant l'installation du nœud)**:["Créez des fichiers de configuration de nœud"](#)
 - **Linux (après l'installation du nœud)**:["Ajouter des interfaces de jonction ou d'accès à un nœud"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#) .

Créez une interface VLAN

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Une interface de ligne réseau a été configurée sur le réseau et connectée au VM ou au nœud Linux. Vous connaissez le nom de l'interface de ligne réseau.
- Vous connaissez l'ID du VLAN que vous configurez.

Description de la tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs VLAN pour isoler le trafic client ou administrateur appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un ID numérique ou une balise. Par exemple, votre réseau peut utiliser le VLAN 100 pour le trafic FabricPool et le VLAN 200 pour une application d'archivage.

Vous pouvez utiliser Grid Manager pour créer des interfaces VLAN qui permettent aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID VLAN et sélectionnez des interfaces parent (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

Étapes

1. Sélectionnez **Configuration > Réseau > Interfaces VLAN**.
2. Sélectionnez **Créer**.

Entrez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN de votre réseau. Vous pouvez entrer n'importe quelle valeur comprise entre 1 et 4094.

Les ID VLAN n'ont pas besoin d'être uniques. Par exemple, vous pouvez utiliser l'ID VLAN 200 pour le trafic administratif sur un site et le même ID VLAN pour le trafic client sur un autre site. Vous pouvez créer des interfaces VLAN distinctes avec différents ensembles d'interfaces parent sur chaque site. Cependant, deux interfaces VLAN avec le même ID ne peuvent pas partager la même interface sur un nœud. Si vous spécifiez un ID déjà utilisé, un message s'affiche.

2. Vous pouvez également saisir une brève description de l'interface VLAN.
3. Sélectionnez **Continuer**.

Choisissez les interfaces parents

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et de passerelle de chaque site de votre grille. Les interfaces Admin Network (eth1) ne peuvent pas être utilisées comme interfaces parents et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parent à laquelle relier ce VLAN.

Par exemple, il peut être nécessaire de connecter un VLAN à l'interface eth2 (client Network) pour un nœud de passerelle et un nœud d'administration.

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.

	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**.

Confirmez les paramètres

Étapes

1. Passez en revue la configuration et apportez les modifications nécessaires.
 - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **entrer les détails du VLAN** en haut de la page.
 - Si vous devez modifier une interface parent, sélectionnez **Choisissez les interfaces parent** en haut de la page ou sélectionnez **Précédent**.
 - Si vous devez supprimer une interface parente, sélectionnez l'icône de 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 (**Nœuds > nœud d'interface parent > Réseau**).

Modifiez une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID ou la description du VLAN.
- Ajouter ou supprimer des interfaces parent.

Par exemple, vous pouvez vouloir supprimer une interface parent d'une interface VLAN si vous envisagez de désaffecter le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID de VLAN si l'interface VLAN est utilisée dans un groupe haute disponibilité.
- Vous ne pouvez pas supprimer une interface parent si cette interface parent est utilisée dans un groupe haute disponibilité.

Par exemple, supposons que le VLAN 200 est connecté aux interfaces parents sur les nœuds A et B. si un groupe haute disponibilité utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parent inutilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parent utilisée pour le nœud A.

Étapes

1. Sélectionnez **Configuration > Réseau > Interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN à modifier. Sélectionnez ensuite **actions > Modifier**.
3. Vous pouvez également mettre à jour l'ID VLAN ou la description. Sélectionnez ensuite **Continuer**.

Vous ne pouvez pas mettre à jour un ID VLAN si ce dernier est utilisé dans un groupe haute disponibilité.

4. Si vous le souhaitez, cochez ou décochez les cases pour ajouter des interfaces parent ou supprimer des interfaces inutilisées. Sélectionnez ensuite **Continuer**.
5. Passez en revue la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprime une interface VLAN

Vous pouvez supprimer une ou plusieurs interfaces VLAN.

Vous ne pouvez pas supprimer une interface VLAN si elle est actuellement utilisée dans un groupe haute disponibilité. Vous devez supprimer l'interface VLAN du groupe haute disponibilité avant de pouvoir le supprimer.

Pour éviter toute perturbation du trafic client, envisagez d'effectuer l'une des opérations suivantes :

- Ajoutez une nouvelle interface VLAN au groupe haute disponibilité avant de supprimer cette interface VLAN.
- Créez un nouveau groupe haute disponibilité qui n'utilise pas cette interface VLAN.
- Si l'interface VLAN que vous souhaitez supprimer est actuellement l'interface active, modifiez le groupe HA. Déplacez l'interface VLAN que vous souhaitez supprimer au bas de la liste des priorités. Attendez que la communication soit établie sur la nouvelle interface principale, puis retirez l'ancienne interface du groupe haute disponibilité. Enfin, supprimez l'interface VLAN de ce nœud.

Étapes

1. Sélectionnez **Configuration > Réseau > Interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN à supprimer. Sélectionnez ensuite **actions > Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

Toutes les interfaces VLAN sélectionnées sont supprimées. Une bannière de réussite verte apparaît sur la page interfaces VLAN.

Activer StorageGRID CORS pour une interface de gestion

En tant qu'administrateur de grille, vous pouvez activer le partage de ressources inter-origines (CORS) pour les demandes d'API de gestion vers StorageGRID, si vous souhaitez que les données de StorageGRID soient accessibles à l'aide des API de gestion vers un autre domaine.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Le ["Autorisation d'accès racine"](#) donne accès à toutes les demandes de configuration CORS.

Description de la tâche

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 souhaitiez créer un tableau de bord de surveillance pour StorageGRID dans le domaine `http://www.example.com`. En activant CORS dans StorageGRID pour `http://www.example.com` et « Grid Manager », le domaine StorageGRID répond aux requêtes de l'API Grid Management de `http://www.example.com`.

Requêtes API de gestion (mgmt-api) avec `application/json` ou `multipart/formdata` demandes de `Content-Type` sont pris en charge pour CORS.

Étapes

1. Dans Grid Manager, accédez à **CONFIGURATION > Réseau > Paramètres CORS de l'interface de**

gestion.

2. Sélectionnez **Grid Manager**, **Tenant Manager** ou les deux options.
 - **Grid Manager** : active CORS pour les requêtes API de gestion de grille inter-domaines.
 - **Gestionnaire de locataires** : active CORS pour les demandes d'API de gestion des locataires inter-domaines.
3. Saisissez l'URL de l'autre domaine dans le champ **Domaines**.

Sélectionnez **Ajouter un autre domaine** si vous souhaitez activer CORS dans StorageGRID pour plusieurs domaines.

4. Sélectionnez **Enregistrer**.

Informations associées

["Configurer StorageGRID CORS pour les buckets et les objets"](#)

Gérer les stratégies de classification du trafic

Politiques de classification du trafic dans StorageGRID

Les stratégies de classification du trafic vous permettent d'identifier et de surveiller différents types de trafic réseau. Ces règles contribuent au contrôle et à la limitation du trafic pour améliorer vos offres de qualité de services (QoS).

Les règles de classification du trafic sont appliquées aux terminaux du service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des stratégies de classification de trafic, vous devez avoir déjà créé des points d'extrémité d'équilibreur de charge.

Règles de correspondance

Chaque règle de classification de trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Sous-réseau
- Locataire
- Terminaux d'équilibrage de charge

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la stratégie conformément aux objectifs de la règle. Tout trafic qui correspond à une règle d'une stratégie est géré par cette règle. Inversement, vous pouvez définir des règles qui correspondent à tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

Vous pouvez également ajouter les types de limite suivants à une règle :

- Bande passante de l'agrégat
- Bande passante par demande
- Requêtes simultanées

- Taux de demande

Les valeurs limites sont appliquées par équilibreur de charge. Si le trafic est réparti simultanément sur plusieurs équilibreurs de charge, les débits maximaux totaux sont un multiple des limites de débit que vous spécifiez.



Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante de l'agrégat ou par requête, les requêtes sont traitées au débit que vous avez défini. StorageGRID ne peut imposer qu'une seule vitesse, donc la règle la plus spécifique, selon le type de correspondance, est celle qui est appliquée. La bande passante consommée par la requête n'est pas prise en compte dans le calcul des autres règles de correspondance moins spécifiques contenant des politiques de limite de bande passante de l'agrégat. Pour tous les autres types de limites, les requêtes client sont retardées de 250 millisecondes et reçoivent une réponse 503 Slow Down pour les requêtes qui dépassent une limite définie par une règle correspondante.

Dans le Gestionnaire de grille, vous pouvez consulter les graphiques de trafic et vérifier que les politiques appliquent bien les limites de trafic attendues.

Utilisez les stratégies de classification du trafic avec les contrats de niveau de service

Vous pouvez utiliser des règles de classification du trafic en association avec les limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des spécificités en matière de capacité, de protection des données et de performances.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des règles de classification du trafic pour atteindre les objectifs de performances de chaque niveau de contrat de niveau de service.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Le coût
Or	1 po de stockage autorisé	Règle ILM 3 copies	25 000 demandes/s Bande passante de 5 Go/s (40 Gbit/s)	par mois
Argent	Stockage de 250 To autorisé	Règle ILM 2 copies	10 000 demandes/s Bande passante de 1.25 Go/s (10 Gbit/s)	\$\$ par mois
Bronze	Stockage de 100 To autorisé	Règle ILM 2 copies	5 000 demandes/s Bande passante de 1 Go/s (8 Gbit/s)	\$ par mois

Vous pouvez créer des règles de classification du trafic si vous souhaitez contrôler et éventuellement limiter le trafic réseau par compartiment, Regex de compartiment, CIDR, terminal d'équilibrage de charge ou locataire. Vous pouvez également définir des limites pour une stratégie en fonction de la bande passante, du nombre de demandes simultanées ou du taux de demande.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Vous avez créé tous les noeuds finaux de l'équilibreur de charge que vous souhaitez associer.
- Vous avez créé les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Classification du trafic**.
2. Sélectionnez **Créer**.
3. Entrez un nom et une description (facultatif) pour la stratégie et sélectionnez **Continuer**.

Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

4. Sélectionnez **Ajouter une règle** et spécifiez les détails suivants pour créer une ou plusieurs règles de correspondance pour la stratégie. Toute stratégie que vous créez doit comporter au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels s'applique la règle correspondante. Les types de trafic sont le compartiment, le Regex de compartiment, le CIDR, le terminal d'équilibrage de la charge et le locataire.

Champ	Description
Valeur de correspondance	Entrez la valeur correspondant au type sélectionné. • Compartiment : entrez un ou plusieurs noms de compartiment. • Regex de compartiment : saisissez une ou plusieurs expressions régulières utilisées pour correspondre à un ensemble de noms de compartiment. L'expression régulière n'est pas ancrée. Utilisez l'ancrage ^ pour faire correspondre au début du nom du compartiment et utilisez l'ancrage \$ pour faire correspondre à la fin du nom. La correspondance d'expression régulière prend en charge un sous-ensemble de la syntaxe PCRE (expression régulière compatible Perl). • CIDR : saisissez un ou plusieurs sous-réseaux IPv4, en notation CIDR, qui correspondent au sous-réseau souhaité. • Noeud final de l'équilibreur de charge : sélectionnez un nom de noeud final. Il s'agit des noeuds finaux de l'équilibreur de charge que vous avez définis sur le "Configurer les terminaux de l'équilibreur de charge". • Tenant : le tenant Matching utilise l'ID de clé d'accès. Si la demande ne contient pas d'ID de clé d'accès (par exemple, un accès anonyme), la propriété du compartiment auquel vous accédez est utilisée pour déterminer le locataire.
Comparaison inverse	Si vous voulez faire correspondre tout le trafic réseau <i>except</i> avec la valeur Type et correspondance que vous venez de définir, cochez la case comparaison inverse. Sinon, laissez la case à cocher désactivée. Par exemple, si vous souhaitez que cette stratégie s'applique à tous les noeuds finaux de l'équilibreur de charge sauf un, spécifiez le noeud final de l'équilibreur de charge à exclure et sélectionnez comparaison inverse. Dans le cas d'une règle contenant plusieurs matcheurs où au moins un est un matcher inverse, veillez à ne pas créer une règle qui correspond à toutes les demandes.

- Si vous le souhaitez, sélectionnez **Ajouter une limite** et sélectionnez les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.



StorageGRID collecte des mesures, même si vous n'ajoutez aucune limite, pour vous permettre de comprendre les tendances du trafic.

Champ	Description
Type	Type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le taux de demande. Remarque : vous pouvez créer des stratégies pour limiter la bande passante agrégée ou pour limiter la bande passante par demande. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante de l'agrégat est utilisée, la bande passante par demande n'est pas disponible. Inversement, lorsque la bande passante par demande est utilisée, la bande passante de l'agrégat n'est pas disponible. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la règle qui correspond le mieux au type de limite défini. Par exemple, si vous avez une stratégie qui limite le trafic dans une seule direction, alors le trafic dans la direction opposée sera illimité, même s'il y a un trafic qui correspond à des stratégies supplémentaires qui ont des limites de bande passante. StorageGRID met en œuvre les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (/32 masque) • Nom exact du compartiment • Seau regex • Locataire • Point final • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Indique si cette limite s'applique aux demandes de lecture client (GET ou HEAD) ou aux demandes d'écriture (PUT, POST ou DELETE).
Valeur	Valeur à laquelle le trafic réseau sera limité, en fonction de l'unité sélectionnée. Par exemple, entrez 10 et sélectionnez MIB/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. Remarque : selon le réglage des unités, les unités disponibles seront soit binaires (par exemple, Gio), soit décimales (par exemple, GB). Pour modifier le paramètre unités, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez Préférences utilisateur.
Unité	Unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de 4 Go/s pour un niveau SLA, créez deux limites de bande passante agrégées : GET/HEAD à 4 Go/s et PUT/POST/DELETE à 4 Go/s.

6. Sélectionnez **Continuer**.

7. Lisez et passez en revue la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la stratégie, sélectionnez **Enregistrer et continuer**.

Le trafic client S3 est désormais géré conformément à la règle de classification du trafic.

Une fois que vous avez terminé

["Afficher les données de trafic réseau"](#) pour vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Modifier une politique de classification du trafic StorageGRID

Vous pouvez modifier une stratégie de classification de trafic pour modifier son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites de la stratégie.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans un tableau.

2. Modifiez la stratégie à l'aide du menu actions ou de la page de détails. Reportez-vous à la section ["créez des stratégies de classification du trafic"](#) pour savoir ce que vous devez saisir.

Menu actions

- a. Cochez la case correspondant à la règle.
- b. Sélectionnez **actions > Modifier**.

Page de détails

- a. Sélectionnez le nom de la stratégie.
- b. Sélectionnez le bouton **Modifier** en regard du nom de la stratégie.

3. Pour l'étape entrer le nom de la stratégie, modifiez éventuellement le nom ou la description de la stratégie et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez éventuellement une règle ou modifiez **Type** et **valeur de correspondance** de la règle existante, puis sélectionnez **Continuer**.
5. Pour l'étape définir les limites, ajoutez, modifiez ou supprimez une limite, et sélectionnez **Continuer**.
6. Consultez la stratégie mise à jour et sélectionnez **Enregistrer et continuer**.

Les modifications apportées à la stratégie sont enregistrées et le trafic réseau est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Supprimer une politique de classification du trafic StorageGRID

Vous pouvez supprimer une stratégie de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la stratégie appropriée car une stratégie ne peut pas être récupérée lorsqu'elle est supprimée.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page stratégies de classification du trafic s'affiche avec les stratégies existantes répertoriées dans un tableau.

2. Supprimez la stratégie à l'aide du menu actions ou de la page de détails.

Menu actions

- a. Cochez la case correspondant à la règle.
- b. Sélectionnez **actions > Supprimer**.

Page de détails de la police

- a. Sélectionnez le nom de la stratégie.
- b. Sélectionnez le bouton **Supprimer** en regard du nom de la stratégie.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la stratégie.

La stratégie est supprimée.

Afficher les indicateurs de trafic réseau dans StorageGRID

Vous pouvez surveiller le trafic réseau en affichant les graphiques disponibles à partir de la page stratégies de classification du trafic.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine ou de comptes de locataires"](#).

Description de la tâche

Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service d'équilibrage de charge pour déterminer si la règle limite avec succès le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la règle.

Même si aucune limite n'est définie pour une stratégie de classification du trafic, des mesures sont recueillies et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la stratégie de classification de trafic pour laquelle vous souhaitez afficher les mesures.

3. Sélectionnez l'onglet **Metrics**.

Les graphiques de stratégie de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

Les graphiques suivants sont inclus sur la page.

- Taux de demande : ce graphique indique la quantité de bande passante correspondant à cette règle gérée par tous les équilibres de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.



Lorsque les demandes sont terminées, ce graphique indique uniquement l'utilisation de la bande passante. Pour les demandes d'objets lents ou volumineux, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

- Taux de réponse aux erreurs : ce graphique fournit une fréquence approximative à laquelle les demandes correspondant à cette stratégie renvoient des erreurs (code d'état HTTP ≥ 400) aux clients.
 - Durée moyenne des demandes (sans erreur) : ce graphique fournit une durée moyenne des demandes réussies correspondant à cette stratégie.
 - Utilisation de la bande passante de la règle : ce graphique indique la quantité de bande passante correspondant à cette règle gérée par tous les équilibres de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.
4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Grasana Dashboard** juste en dessous du titre Metrics pour afficher tous les graphiques d'une police. En plus des quatre graphiques de l'onglet **Metrics**, vous pouvez afficher deux autres graphiques :
- Taux de demande d'écriture par taille d'objet : taux pour les demandes PUT/POST/DELETE correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.
 - Taux de demande de lecture par taille d'objet : taux des demandes GET/HEAD correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.
6. Vous pouvez également accéder aux graphiques depuis le menu **Support**.
- a. Sélectionnez **Support > Outils > Métriques**.

- b. Sélectionnez **politique de classification du trafic** dans la section **Grafana**.
- c. Sélectionnez la stratégie dans le menu en haut à gauche de la page.
- d. Placez le curseur sur un graphique pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objet agrégées dans le nombre et le nombre de demandes par seconde pendant cette période.

Les politiques de classification du trafic sont identifiées par leur ID. Les ID de stratégie sont répertoriés sur la page règles de classification de trafic.

7. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Chiffrements pris en charge pour les connexions TLS sortantes dans StorageGRID

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (transport Layer Security) avec les systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Versions supportées de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Les chiffrements TLS 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 ingénieur commercial NetApp pour toute demande spécifique concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées dans StorageGRID

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages de maintenir les connexions HTTP inactives ouvertes

Gardez les connexions HTTP ouvertes lorsque les applications clientes sont inactives pour permettre des transactions ultérieures. Gardez une connexion HTTP inactive ouverte pendant 10 minutes maximum.

StorageGRID peut fermer automatiquement une connexion HTTP ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

La réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Décidez combien de temps maintenir une connexion inactive ouverte en équilibrant les avantages du démarrage lent et l'allocation des ressources.

Avantages des connexions HTTP actives

Pour les connexions directes aux nœuds de stockage, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue des transactions en continu.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

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 cette méthode annule les gains précieux associés aux connexions persistantes.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

Les transactions peuvent commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

La topologie de chaque système StorageGRID présente un débit maximal différent pour les transactions et les connexions simultanées. Le débit maximal dépend des ressources de calcul, du réseau, de stockage, des liaisons WAN et du nombre de serveurs, de services et d'applications pris en charge par le système StorageGRID .

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Gardez cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées. Si l'application cliente se compose de plusieurs entités logicielles qui établissent chacune des connexions au système StorageGRID , additionnez 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 pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.
- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.

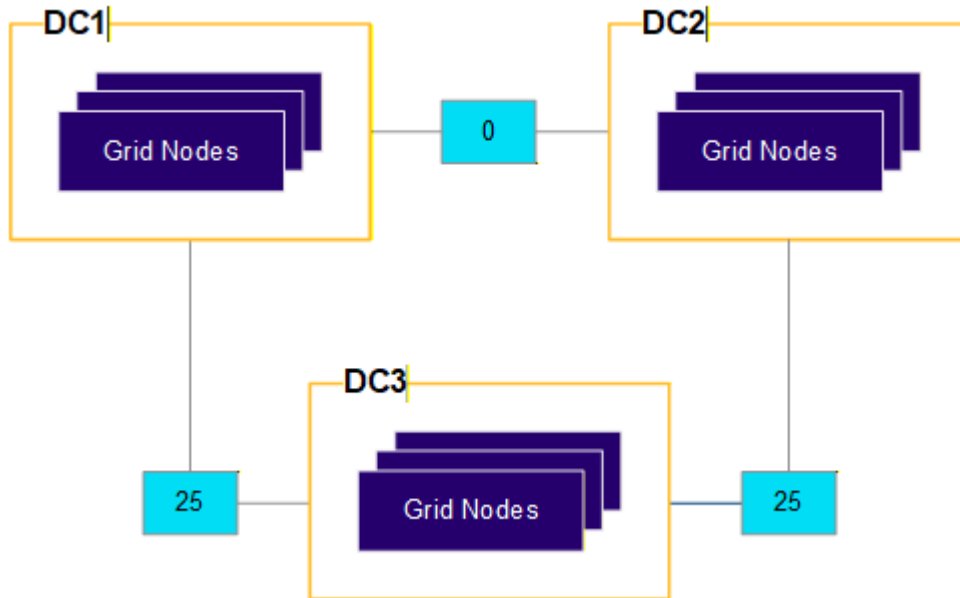
Gérer les coûts de liaison dans StorageGRID

Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts des liens permettent de classer par ordre de priorité la copie d'objet utilisée pour les récupérations d'objets.
- Les coûts des liaisons sont utilisés par l'API de gestion du grid et l'API de gestion des locataires pour déterminer quels services StorageGRID internes utiliser.
- Le service d'équilibrage de charge utilise les coûts de liaison sur les nœuds d'administration et les nœuds de passerelle pour diriger les connexions client. Reportez-vous à "[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 Load Balancer sur les nœuds d'administration et les nœuds de passerelle répartit uniformément les connexions client vers tous les nœuds de stockage sur le même site de data Center et vers tous les sites de data Center, avec un coût de liaison de 0.

Dans l'exemple, un nœud passerelle du site de data Center 1 (DC1) distribue également les connexions client aux nœuds de stockage du DC1 et aux nœuds de stockage du DC2. Un nœud de passerelle du DC3 envoie des connexions client uniquement aux nœuds de stockage du DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie au niveau du data Center présentant le coût de liaison le plus faible.

Dans cet exemple, si une application client sur DC2 récupère un objet stocké à la fois sur DC1 et DC3, l'objet est récupéré de DC1, car le coût de la liaison de DC1 à DC2 est 0, ce qui est inférieur au coût de la liaison de DC3 à DC2 (25).

Les coûts de liaison sont des nombres relatifs arbitraires sans unité de mesure spécifique. Par exemple, un coût de lien de 50 est utilisé de manière moins préférentielle qu'un coût de lien de 25. Le tableau indique les coûts de liaison couramment utilisés.

Lien	Coût des liens	Remarques
Entre les sites de data centers physiques	25 (par défaut)	Data centers connectés par une liaison WAN.
Entre des sites de data centers logiques au même emplacement physique	0	Data centers logiques dans le même bâtiment physique ou campus connecté par un réseau LAN.

Mettre à jour les coûts des liens

Vous pouvez mettre à jour les coûts de liaison entre les sites de data Center afin de refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Assistance > Autre > Coût du lien**.
2. Pour chaque site listé dans la colonne Coût du site/lien, saisissez une valeur de coût de 0 à 100 pour les autres sites.

Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

3. Annuler ou enregistrer les modifications :
 - Pour annuler les modifications, sélectionnez **Effacer les modifications**.
 - Pour enregistrer les modifications, sélectionnez **Enregistrer**.

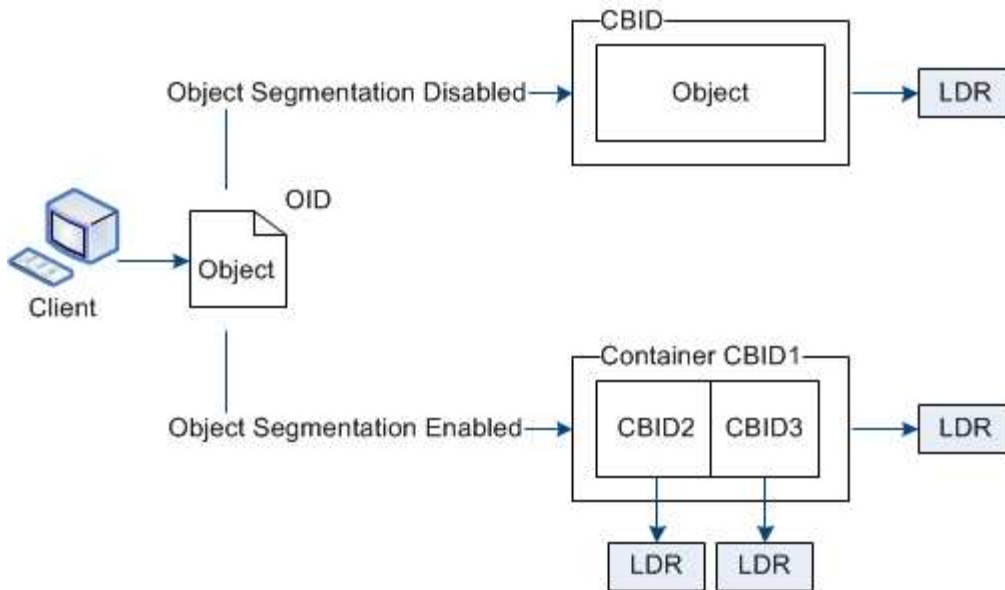
Gérer des nœuds de stockage

Utilisez les options de stockage

Découvrez la segmentation des objets dans StorageGRID

La segmentation d'objet consiste à diviser un objet en un ensemble d'objets de taille fixe plus petits afin d'optimiser l'utilisation du stockage et des ressources pour les objets de grande taille. Le téléchargement multi-pièces S3 crée également des objets segmentés, avec un objet représentant chaque pièce.

Lorsqu'un objet est ingéré dans le système StorageGRID, le service LDR divise l'objet en segments et crée un conteneur de segments qui répertorie les informations d'en-tête de tous les segments en tant que contenu.



Lors de la récupération d'un conteneur de segments, le service LDR assemble l'objet original à partir de ses segments et renvoie l'objet au client.

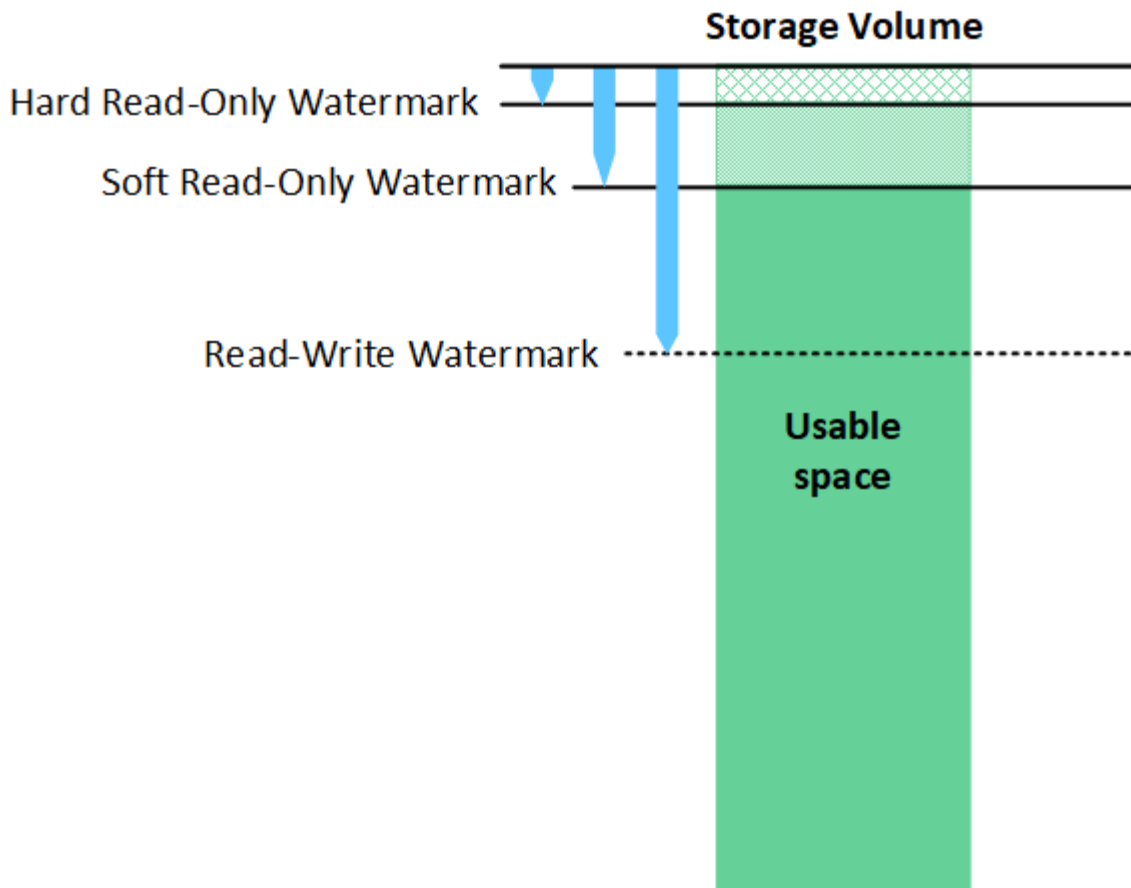
Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Les conteneurs et les segments peuvent être stockés sur n'importe quel nœud de stockage du pool de stockage spécifié dans la règle ILM.

Chaque segment est traité indépendamment par le système StorageGRID et contribue au nombre d'attributs tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID est divisé en deux segments, la valeur des objets gérés augmente de trois après la fin de l'acquisition, comme suit :

```
segment container + segment 1 + segment 2 = three stored objects
```

Découvrez les seuils de volume de stockage dans StorageGRID

StorageGRID utilise trois filigranes de volume de stockage qui garantissent que les nœuds de stockage sont transférés en toute sécurité vers un état en lecture seule avant de s'exécuter avec un espace critique et que les nœuds de stockage ayant été transférés vers un état en lecture seule afin de devenir à nouveau en lecture/écriture.



Les filigranes du volume de stockage ne s'appliquent qu'à l'espace utilisé pour les données d'objets répliqués et codés par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées d'objet sur le volume 0, rendez-vous "[Gérer le stockage des métadonnées d'objet](#)" sur .

Qu'est-ce que le filigrane logiciel en lecture seule ?

Le filigrane **soft read-only du volume de stockage** est le premier filigrane qui indique que l'espace utilisable d'un nœud de stockage pour les données d'objet est saturé.

Si chaque volume d'un nœud de stockage dispose d'un espace libre inférieur au 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 des services en lecture seule au reste du système StorageGRID, mais remplit toutes les demandes d'écriture en attente.

Supposons, par exemple, que chaque volume d'un nœud de stockage possède un filigrane en lecture seule de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode veille souple en lecture seule.

Qu'est-ce que le filigrane en lecture seule ?

Le filigrane **en lecture seule du volume de stockage** est le filigrane suivant pour indiquer que l'espace utilisable d'un nœud pour les données d'objet est saturé.

Si l'espace disponible sur un volume est inférieur au filigrane en lecture seule, les écritures sur le volume échoueront. Cependant, les écritures sur d'autres volumes peuvent se poursuivre jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leurs filigranes en lecture seule.

Supposons, par exemple, que chaque volume d'un nœud de stockage 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 de demandes d'écriture.

Le filigrane en lecture seule est toujours inférieur au filigrane en lecture seule.

Qu'est-ce que le filigrane de lecture-écriture ?

Le filigrane **lecture-écriture du volume de stockage** ne s'applique qu'aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine quand le nœud peut redevenir lecture-écriture. Lorsque l'espace libre sur un volume de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud revient automatiquement à l'état de lecture-écriture.

Supposons par exemple que le nœud de stockage est passé en mode lecture seule. Supposons également que chaque volume possède un filigrane de lecture-écriture de 30 Go. Dès que l'espace libre d'un volume augmente jusqu'à 30 Go, le nœud redevient read-write.

Le filigrane en lecture-écriture est toujours plus grand que le filigrane en lecture seule et le filigrane en lecture seule.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres actuels du filigrane ainsi que les valeurs optimisées par le système. Si les filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez régler les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Afficher les paramètres actuels du filigrane

Vous pouvez afficher les paramètres actuels du filigrane de stockage dans Grid Manager.

Étapes

1. Sélectionnez **Assistance > Autre > Filigranes de stockage**.
2. Sur la page filigranes de stockage, cochez la case utiliser les valeurs optimisées.
 - Si cette case est cochée, 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 des filigranes de stockage optimisés](#).

- Si la case utiliser les valeurs optimisées n'est pas cochée, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Suivez les instructions de ["Dépannage des alertes de remplacement du filigrane en lecture seule faible"](#) pour déterminer si vous pouvez ou devez régler les paramètres.

Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez entrer des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le seuil en lecture seule souple du volume de stockage. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

1. Sélectionnez **Support > Outils > Métriques**.
2. Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
3. Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé du filigrane en lecture seule du volume de stockage, l'alerte **Low read-only filigrane override** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

Gérez le stockage des métadonnées des objets dans StorageGRID

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets qui peuvent être stockés sur le système en question. Pour s'assurer que votre système StorageGRID dispose d'un espace suffisant pour stocker les nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées d'objet.

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

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

Pour un objet dans StorageGRID, les métadonnées d'objet incluent les types d'information suivants :

- Métadonnées du 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 création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du

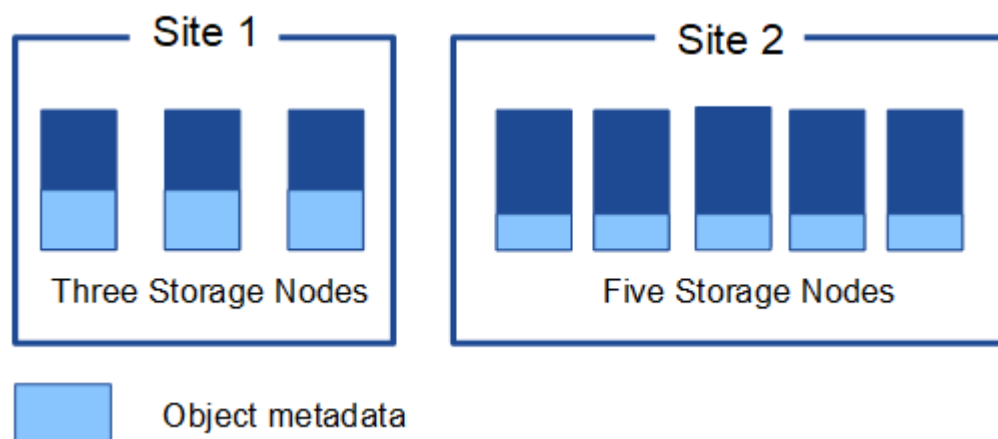
compartiment externe et l'identifiant unique de l'objet.

- Pour les objets segmentés et les objets à plusieurs parties, les identificateurs de segment et la taille des données.

Comment les métadonnées d'objet sont-elles stockées ?

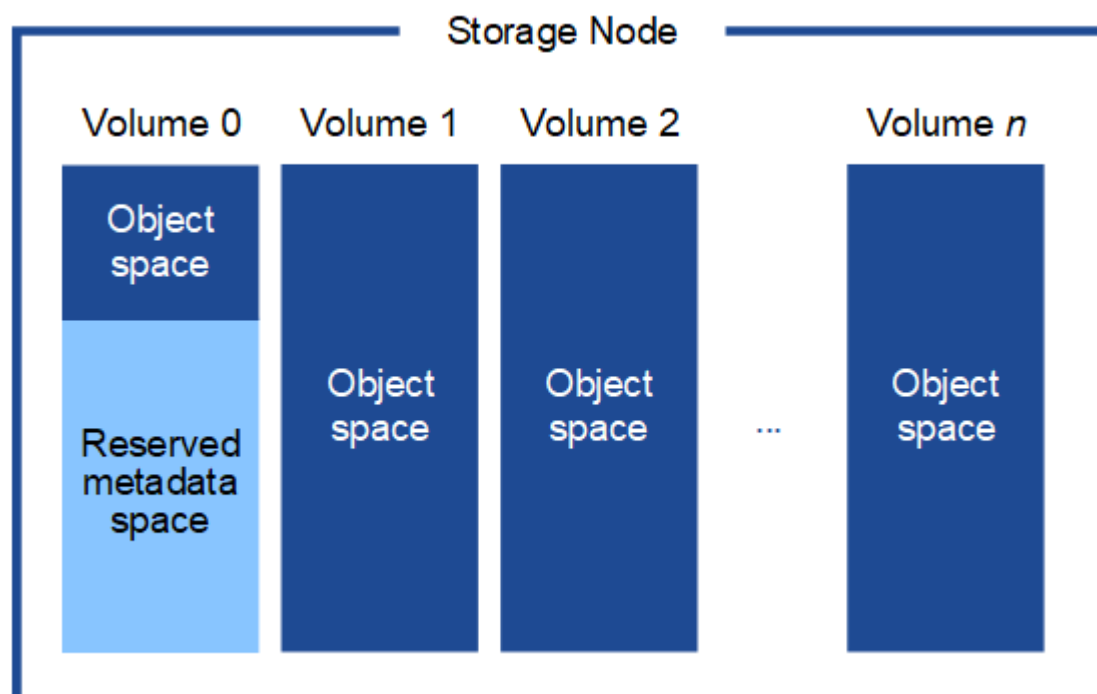
Les métadonnées d'objet sont conservées dans une base de données Cassandra, stockée indépendamment des données d'objet. StorageGRID Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site dispose du même volume de métadonnées objet, et les métadonnées de chaque site sont subdivisées en plusieurs nœuds de stockage sur ce site.



Où sont stockées les métadonnées d'objet ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées d'objet et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments avec code d'effacement).

La quantité d'espace réservée aux métadonnées d'objet sur un nœud de stockage particulier dépend de plusieurs facteurs, décrits ci-dessous.

Paramètre d'espace réservé de 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 utilisez lors de l'installation initiale de StorageGRID.
- Quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé par défaut pour les métadonnées
12,1	Au moins 128 Go sur chaque nœud de stockage de la grille	20 To (20 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage de la grille	3 TO (3,000 GO)
11,5 à 12,0	Au moins 128 Go sur chaque nœud de stockage de la grille	8 TO (8,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de la grille	3 TO (3,000 GO)
11.1 à 11.4	128 Go ou plus sur chaque nœud de stockage sur un site	4 TO (4,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de chaque site	3 TO (3,000 GO)
11.0 ou antérieure	Tout montant	2 TO (2,000 GO)

Afficher le paramètre d'espace réservé aux métadonnées

Procédez comme suit pour afficher le paramètre espace réservé aux métadonnées de 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 version ultérieure, la valeur de l'espace réservé aux métadonnées doit être d'au moins 100 Go et d'au plus 1 po.

La configuration par défaut pour une nouvelle installation StorageGRID 12.1 ou supérieure dans laquelle chaque nœud de stockage dispose de 128 Go ou plus de RAM est de 20 000 Go (20 To).

Espace réservé réel pour les métadonnées

Contrairement au paramètre espace réservé pour les métadonnées à l'échelle du système, l'espace réservé *réel* pour les métadonnées de l'objet est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre d'espace réservé pour les métadonnées à l'échelle du système.

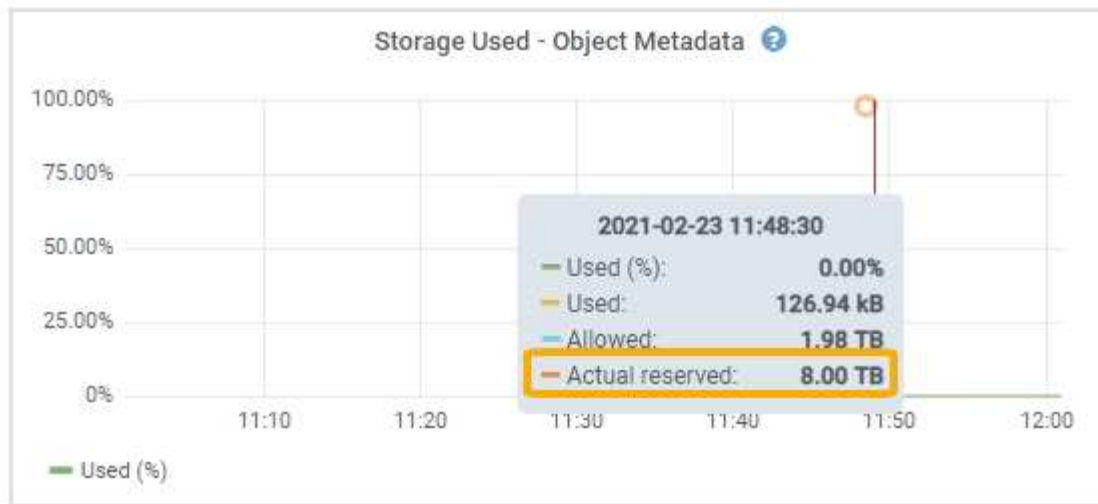
Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (utilisation hors production)	10 % du volume 0
500 Go ou plus + ou + nœuds de stockage des métadonnées uniquement	Plus ces valeurs sont faibles : • Volume 0 • Paramètre d'espace réservé de métadonnées Remarque : un seul rangedb est requis pour les nœuds de stockage de métadonnées uniquement.

Afficher l'espace réservé réel pour les métadonnées

La procédure suivante permet d'afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **Nœuds > Nœud de stockage**.
2. Sélectionnez l'onglet **stockage**.
3. Placez votre curseur sur le graphique stockage utilisé - métadonnées de l'objet et localisez la valeur **réel réservé**.



Sur la capture d'écran, la valeur réservée réelle est de 20 To. Cette capture d'écran concerne un grand nœud de stockage dans une nouvelle installation StorageGRID 12.1. Le volume 0 a une capacité d'au moins 20 To, il utilise donc le paramètre d'espace réservé aux métadonnées par défaut à l'échelle du système.

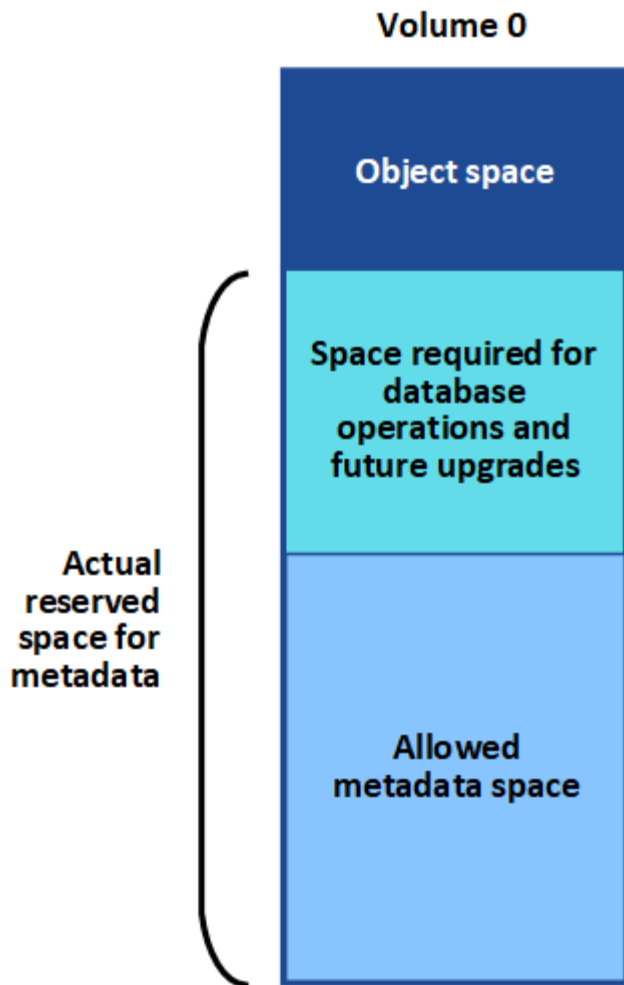
Exemple d'espace de métadonnées réellement réservé

Supposons que vous installiez un nouveau système StorageGRID en utilisant la version 12.1 ou ultérieure. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 20 To. (Il s'agit de la valeur par défaut pour une nouvelle installation de StorageGRID 12.1 ou supérieure si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace **réellement réservé** pour les métadonnées de 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 divisé en l'espace disponible pour les métadonnées d'objet (l'espace *autorisé metadata space*) et l'espace requis pour les opérations essentielles de bases de données (telles que la compaction et la réparation) et les mises à niveau matérielles et logicielles futures. L'espace de métadonnées autorisé régit la capacité globale des objets.



Le tableau suivant montre comment StorageGRID calcule l' **espace de métadonnées autorisé** pour différents nœuds de stockage, en fonction de la quantité de mémoire du nœud et de l'espace réservé réel pour les métadonnées.

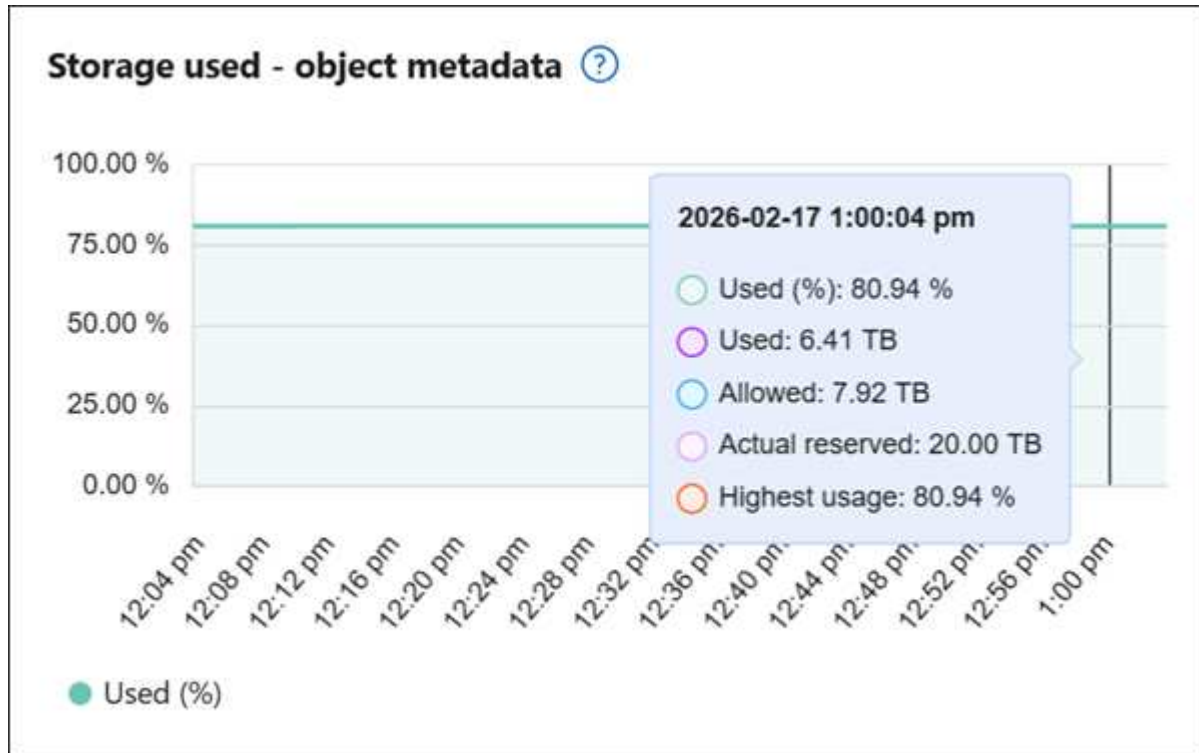
		Quantité de mémoire sur le nœud de stockage	
	< 128 GB	≥ 128 Go	Espace réservé réel pour les métadonnées
< 4 To	75 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,32 To	75 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,98 To	≥ 4 To

Afficher l'espace de métadonnées autorisé

La procédure suivante permet d'afficher l'espace de métadonnées autorisé pour un nœud de stockage.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **Nœuds**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **stockage**.
4. Placez votre curseur sur le graphique de métadonnées de l'objet stockage utilisé - et localisez la valeur **autorisé**.



Sur la capture d'écran, la valeur **Allowed** est de 7,92 To, ce qui correspond à la valeur maximale pour un Storage Node dont l'espace réellement réservé aux métadonnées est supérieur à 4 To.

La valeur **autorisé** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installiez un nouveau système StorageGRID en utilisant la version 12.1 ou ultérieure. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 20 To. (Il s'agit de la valeur par défaut pour une nouvelle installation de StorageGRID 12.1 ou supérieure si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace **réellement réservé** pour les métadonnées de 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 3,75 To, basé sur le calcul indiqué dans le [tableau pour l'espace autorisé pour les métadonnées](#) : (Espace réellement réservé pour les métadonnées – 1 To) × 75 %, jusqu'à un maximum de 7,92 To.

La façon dont les nœuds de stockage de différentes tailles affectent la capacité des objets

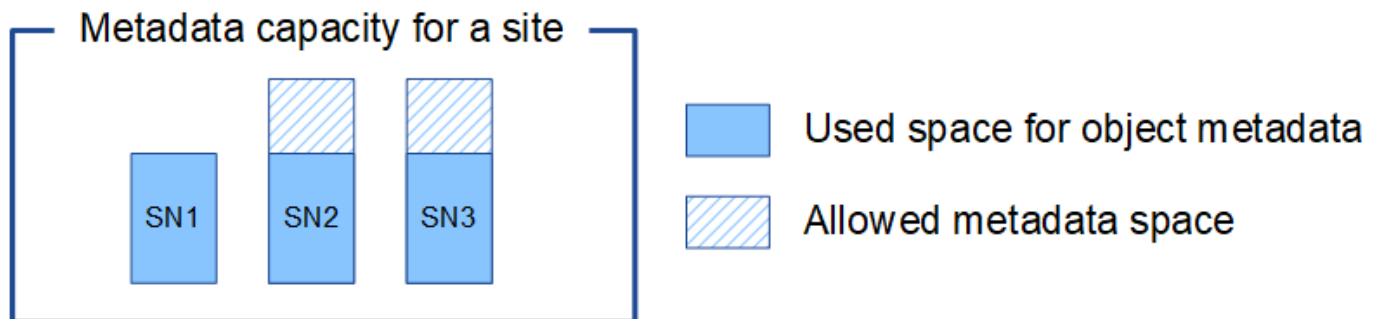
Comme décrit ci-dessus, StorageGRID distribue uniformément les métadonnées d'objet sur les nœuds de stockage sur chaque site. Par conséquent, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité des métadonnées du site.

Prenons l'exemple suivant :

- Une grille sur un seul site contient trois nœuds de stockage de tailles différentes.
- Le paramètre **espace réservé aux métadonnées** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace réservé réel des métadonnées et l'espace autorisé pour les métadonnées.

Nœud de stockage	Taille du volume 0	Espace réservé réel des métadonnées	Espace de métadonnées autorisé
SN1	2.2 TO	2.2 TO	1.32 TO
SN2	5 TO	4 TO	1.98 TO
SN3	6 To	4 TO	1.98 TO

Les métadonnées de l'objet sont réparties de manière uniforme sur les nœuds de stockage d'un site. En effet, chaque nœud de cet exemple ne peut contenir que 1.32 To de métadonnées. Les 0.66 To supplémentaires d'espace de métadonnées autorisé pour SN2 et SN3 ne peuvent pas être utilisés.



De même, puisque StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale des métadonnées d'un système StorageGRID est déterminée par la capacité des métadonnées d'objet du plus petit site.

Étant donné que la capacité des métadonnées contrôle le nombre maximal d'objets, lorsqu'un nœud vient à manquer de capacité de métadonnées, la grille est véritablement pleine.

Informations associées

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, reportez-vous aux instructions de la ["Surveillance StorageGRID"](#).
- Pour augmenter la capacité de métadonnées d'objet de votre système, ["développez une grille"](#) ajoutez de nouveaux nœuds de stockage.

Augmentez le paramètre Metadata Reserved Space dans StorageGRID

Vous pouvez augmenter le paramètre système Metadata Reserved Space si vos nœuds de stockage répondent aux exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root ou autre autorisation de configuration de grille"](#).

Description de la tâche

Vous pouvez augmenter manuellement l'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 pour l'ensemble du système que si ces deux instructions sont vraies :

- Les nœuds de stockage de n'importe quel site de votre système disposent chacun d'au moins 128 Go de RAM.
- L'espace disponible des nœuds de stockage de n'importe quel site du système est suffisant pour le volume de stockage 0.

Notez que si vous augmentez ce paramètre, vous réduisez simultanément l'espace disponible pour le stockage objet sur le volume de stockage 0 de tous les nœuds de stockage. C'est pour cette raison que vous préférez définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction des exigences de métadonnées de l'objet que vous prévoyez.



En général, il est préférable d'utiliser une valeur plus élevée au lieu d'une valeur plus faible. Si le paramètre espace réservé aux métadonnées est trop grand, vous pouvez le réduire ultérieurement. Par opposition, si vous augmentez la valeur par la suite, le système peut avoir besoin de déplacer les données d'objet afin de libérer de l'espace.

Pour une explication détaillée de la façon dont le paramètre espace réservé des métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, reportez-vous à la section ["Gérer le stockage des métadonnées d'objet"](#).

Étapes

1. Déterminez le paramètre actuel espace réservé aux métadonnées.
 - a. Sélectionnez **Configuration > Système > Paramètres de stockage**.
 - b. Notez la valeur de **Espace réservé aux métadonnées**.
2. Assurez-vous d'avoir suffisamment d'espace disponible sur le volume de stockage 0 de chaque nœud de stockage pour augmenter cette valeur.
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez le premier nœud de stockage dans la grille.
 - c. Cliquez sur l'onglet stockage.
 - d. Dans la section volumes, recherchez l'entrée **/var/local/rangedb/0**.
 - e. Vérifiez 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 cette procédure pour tous les nœuds de stockage.

- Si un ou plusieurs nœuds de stockage ne disposent pas d'espace disponible suffisant, la valeur espace réservé aux métadonnées ne peut pas être augmentée. Ne pas poursuivre cette procédure.
- Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.

3. Vérifiez que vous disposez d'au moins 128 Go de RAM sur chaque nœud de stockage.

a. Sélectionnez **Nœuds**.

b. Sélectionnez le premier nœud de stockage dans la grille.

c. Sélectionnez l'onglet **matériel**.

d. Placez le curseur sur le graphique utilisation de la mémoire. Vérifiez que **mémoire totale** est d'au moins 128 Go.

e. Répétez cette procédure 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 pas poursuivre cette procédure.
- Si chaque nœud de stockage dispose d'au moins 128 Go de mémoire totale, passez à l'étape suivante.

4. Mettez à jour le paramètre Metadata Reserved Space.

a. Sélectionnez **Configuration > Système > Paramètres de stockage**.

b. Sélectionnez **Espace réservé aux métadonnées**.

c. Entrez la nouvelle valeur.

Par exemple, pour saisir 8 To, qui est la valeur maximale prise en charge, entrez **8000000000000** (8, suivi de 12 zéros).

d. Sélectionnez **Enregistrer**.

Compresser les objets stockés dans StorageGRID

Vous pouvez activer la compression des objets afin de réduire la taille des objets stockés dans StorageGRID, de sorte que les objets consomment moins d'espace de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Description de la tâche

Par défaut, la compression des objets est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement à l'aide de la compression sans perte.



Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Avant d'activer la compression d'objets, tenez compte des points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés**, sauf si vous savez que les données stockées sont compressibles.
- Les applications qui enregistrent des objets dans StorageGRID peuvent compresser les objets avant de les enregistrer. Si une application client a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille d'un objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si **Compress Stored objects** est sélectionné, les applications client S3 doivent éviter d'effectuer des opérations GetObject qui spécifient une plage d'octets. 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 objet très volumineux 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 client peuvent être en attente.



Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Étapes

1. Sélectionnez **Configuration > Système > Paramètres de stockage > Compression d'objet**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer les nœuds de stockage complets dans StorageGRID

Lorsque les nœuds de stockage atteignent leur capacité maximale, ils doivent étendre le système StorageGRID en ajoutant du nouveau stockage. Trois options sont disponibles : ajout de volumes de stockage, ajout de tiroirs d'extension de stockage et ajout de nœuds de stockage.

Ajout de volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plate-forme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximum, vous pouvez ajouter des volumes pour augmenter sa capacité. Voir les instructions pour ["Extension d'un système StorageGRID"](#).

Ajout de tiroirs d'extension de stockage

Certains nœuds de stockage d'appliance StorageGRID, tels que SG6060 ou SG6160, peuvent prendre en charge des tiroirs de stockage supplémentaires. Si vos appliances StorageGRID bénéficient de fonctionnalités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des tiroirs de stockage pour augmenter la capacité. Voir les instructions pour ["Extension d'un système StorageGRID"](#).

Ajouter des nœuds de stockage

L'ajout de nœuds de stockage permet d'augmenter la capacité de stockage. L'ajout de stockage nécessite de

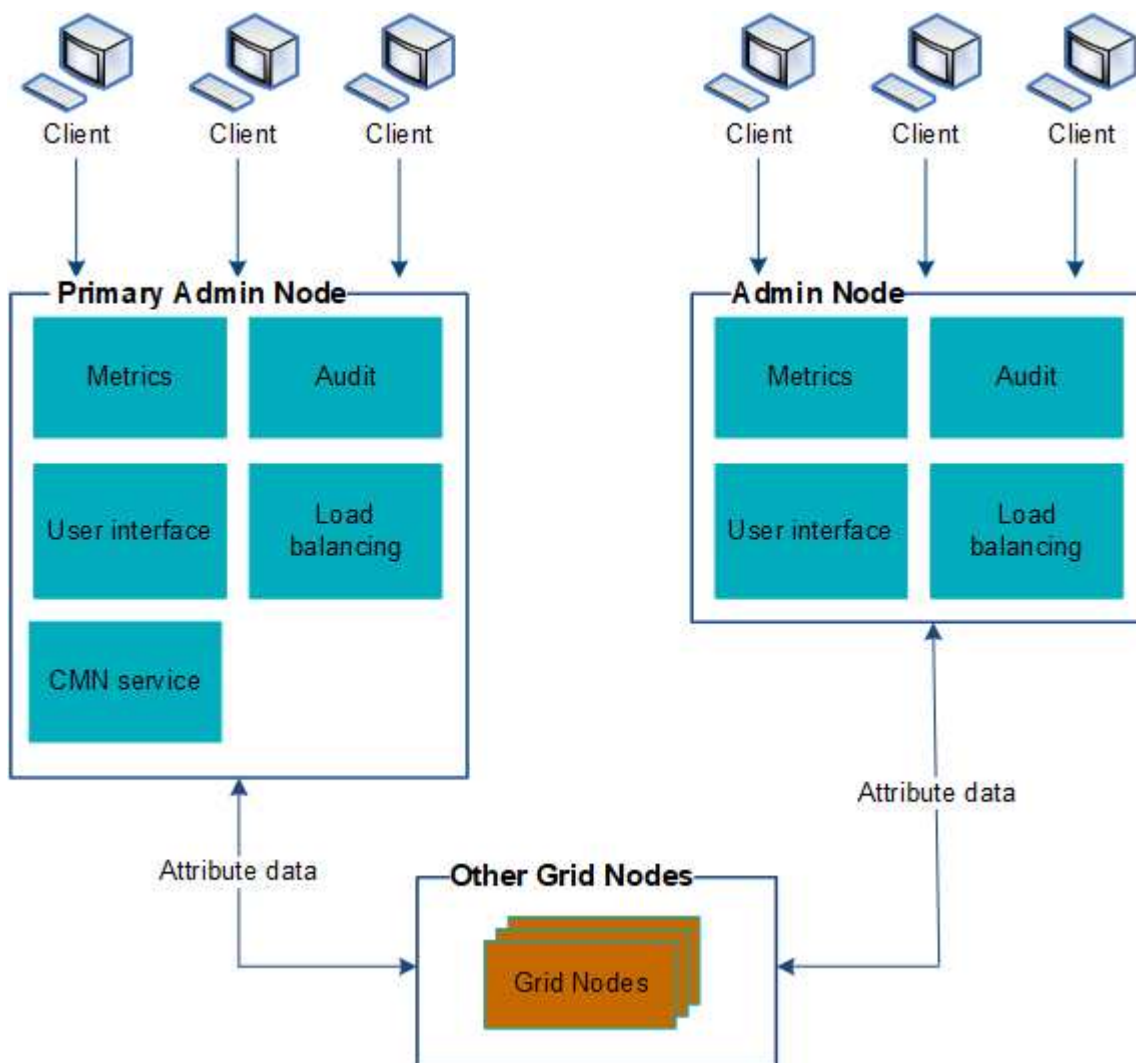
prendre en compte les règles ILM et les exigences de capacité actuellement actives. Voir les instructions pour ["Extension d'un système StorageGRID"](#).

Gérer les nœuds d'administration

Utilisez plusieurs nœuds d'administration dans StorageGRID

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en cas de panne d'un nœud d'administration.

Si un nœud d'administration n'est plus disponible, le traitement des attributs se poursuit, les alertes sont toujours déclenchées et les notifications par e-mail et les packs AutoSupport sont toujours envoyés. Toutefois, le fait d'avoir plusieurs nœuds d'administration n'offre pas de protection de basculement, à l'exception des notifications et des packages AutoSupport.



Deux options s'offrent à vous pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les

clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir ["Gérez les groupes haute disponibilité"](#).



En cas d'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de panne du nœud d'administration actif. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA bascule vers un autre nœud d'administration du groupe.

Certaines tâches de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal. En cas de panne du nœud d'administration principal, celui-ci doit être restauré avant que le système StorageGRID ne fonctionne à nouveau entièrement.

Identifiez le nœud d'administration principal dans StorageGRID

Le nœud d'administration principal offre davantage de fonctionnalités que les nœuds d'administration non primaires. 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, reportez-vous à la section ["Qu'est-ce qu'un nœud d'administration"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **Nœuds**.
2. Entrez **primary** dans la zone de recherche.

Dans les résultats de la recherche, identifiez le nœud avec le « nœud d'administration principal » affiché dans la colonne Type. Un nœud d'administration principal doit être répertorié.

Gestion des objets avec ILM

Gérez les objets avec ILM dans StorageGRID

Les règles de gestion du cycle de vie des informations (ILM) indiquent à StorageGRID comment créer et distribuer des copies de données en mode objet et comment gérer ces copies au fil du temps.

À propos de ces instructions

La conception et l'implémentation de règles et de règles ILM nécessitent une planification rigoureuse. Vous devez connaître vos exigences opérationnelles, la topologie de votre système StorageGRID, vos besoins en matière de protection des objets et les types de stockage disponibles. Ensuite, vous devez déterminer comment vous voulez que différents types d'objets soient copiés, distribués et stockés.

Suivez ces instructions pour :

- En savoir plus sur la solution ILM ["ILM fonctionne tout au long de la vie d'un objet"](#) de StorageGRID, notamment .

- Apprenez à configurer "[pools de stockage](#)", "[Pools de stockage cloud](#)", et "[Règles ILM](#)".
- Découvrez comment "[Créez, simulez et activez une règle ILM](#)" protéger les données d'objet sur un ou plusieurs sites.
- Découvrez comment "[Gestion des objets avec le verrouillage objet S3](#)", qui permet de vous assurer que les objets de compartiments S3 spécifiques ne sont pas supprimés ou remplacés pendant une durée spécifiée.

En savoir plus >>

Pour en savoir plus, consultez ces vidéos :

[Aperçu des règles de l'ILM](#)

[Aperçu des politiques ILM](#)

ILM et cycle de vie des objets

Fonctionnement de l'ILM tout au long du cycle de vie d'un objet dans StorageGRID

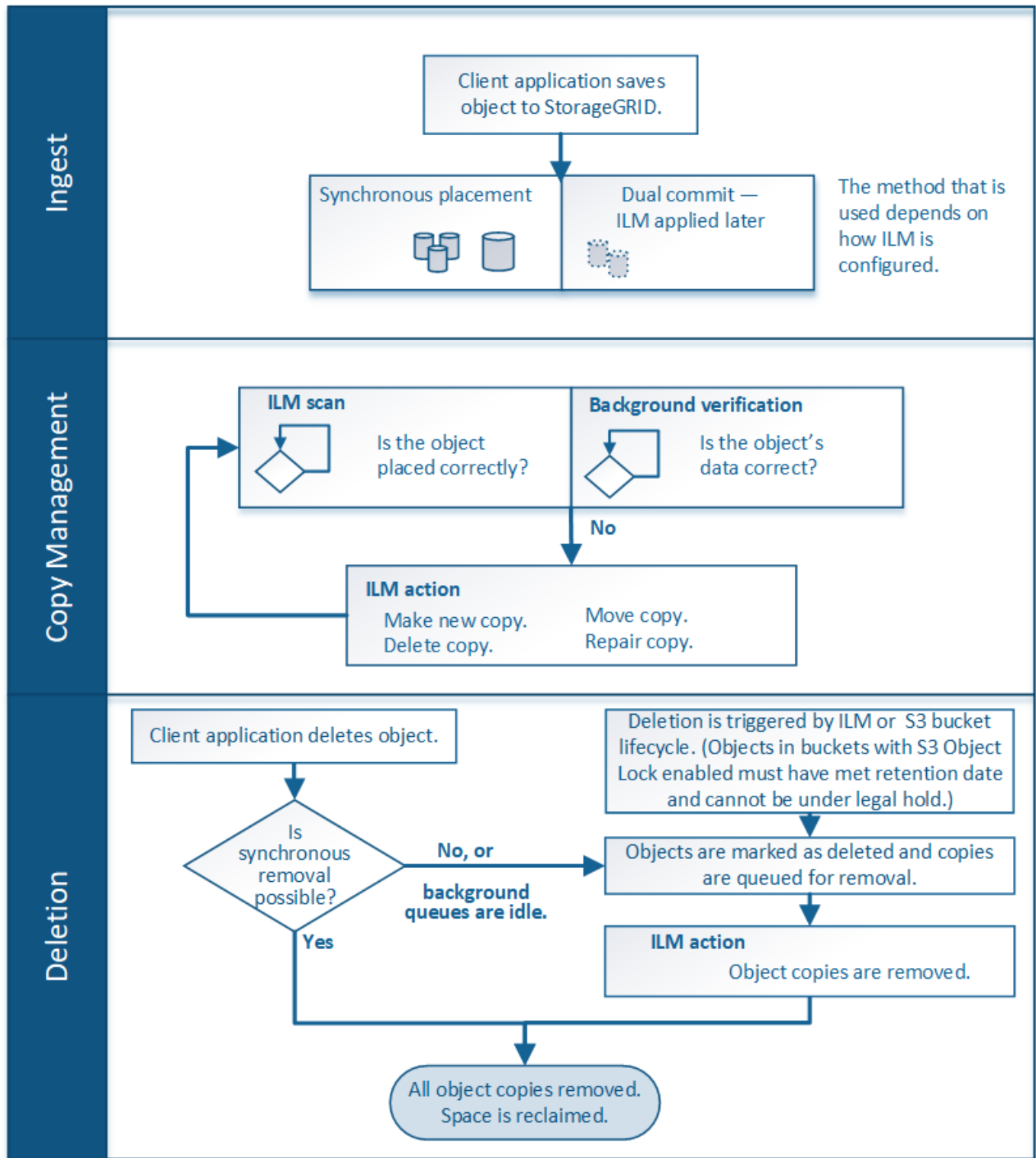
La compréhension de la façon dont StorageGRID utilise les règles ILM pour gérer les objets à chaque étape de leur vie peut vous aider à concevoir des règles plus efficaces.

- **Ingest** : l'acquisition commence lorsqu'une application client S3 établit une connexion pour enregistrer un objet dans le système StorageGRID, et est terminée lorsque StorageGRID renvoie un message « acquisition réussie » au client. Les données d'objet sont protégées pendant l'ingestion, soit par application immédiate d'instructions ILM (placement synchrone), soit par création de copies intermédiaires et application de la règle ILM (double allocation), en fonction de la spécification des exigences ILM.
- **Gestion des copies** : après la création du nombre et du type de copies d'objets spécifiés dans les instructions de placement de l'ILM, StorageGRID gère les emplacements des objets et protège les objets contre les pertes.
 - **Analyse et évaluation ILM** : StorageGRID analyse en continu la liste des objets stockés dans la grille et vérifie si les copies actuelles répondent aux exigences ILM. Lorsque différents types, nombres ou emplacements de copies d'objets sont requis, StorageGRID crée, supprime ou déplace des copies selon les besoins.
 - **Vérification de l'arrière-plan** : StorageGRID effectue en permanence une vérification de l'arrière-plan pour vérifier l'intégrité des données de l'objet. En cas de problème, StorageGRID crée automatiquement une nouvelle copie objet ou un fragment d'objet de code d'effacement de remplacement à un emplacement conforme aux exigences ILM actuelles. Voir "[Vérifiez l'intégrité de l'objet](#)".
- **Suppression d'objet** : la gestion d'un objet se termine lorsque toutes les copies sont supprimées du système StorageGRID. La suppression d'objets peut être due à une demande de suppression d'un client, ou à la suppression d'un ILM ou d'un programme de suppression provoqué par l'expiration du cycle de vie d'un compartiment S3.



Les objets d'un compartiment pour lequel le verrouillage objet S3 est activé ne peuvent pas être supprimés s'ils sont soumis à une conservation légale ou si une date de conservation jusqu'à a été spécifiée, mais pas encore remplie.

Le diagramme résume le fonctionnement de ILM tout au long du cycle de vie d'un objet.



Mode d'ingestion des objets

Options d'ingestion ILM dans StorageGRID

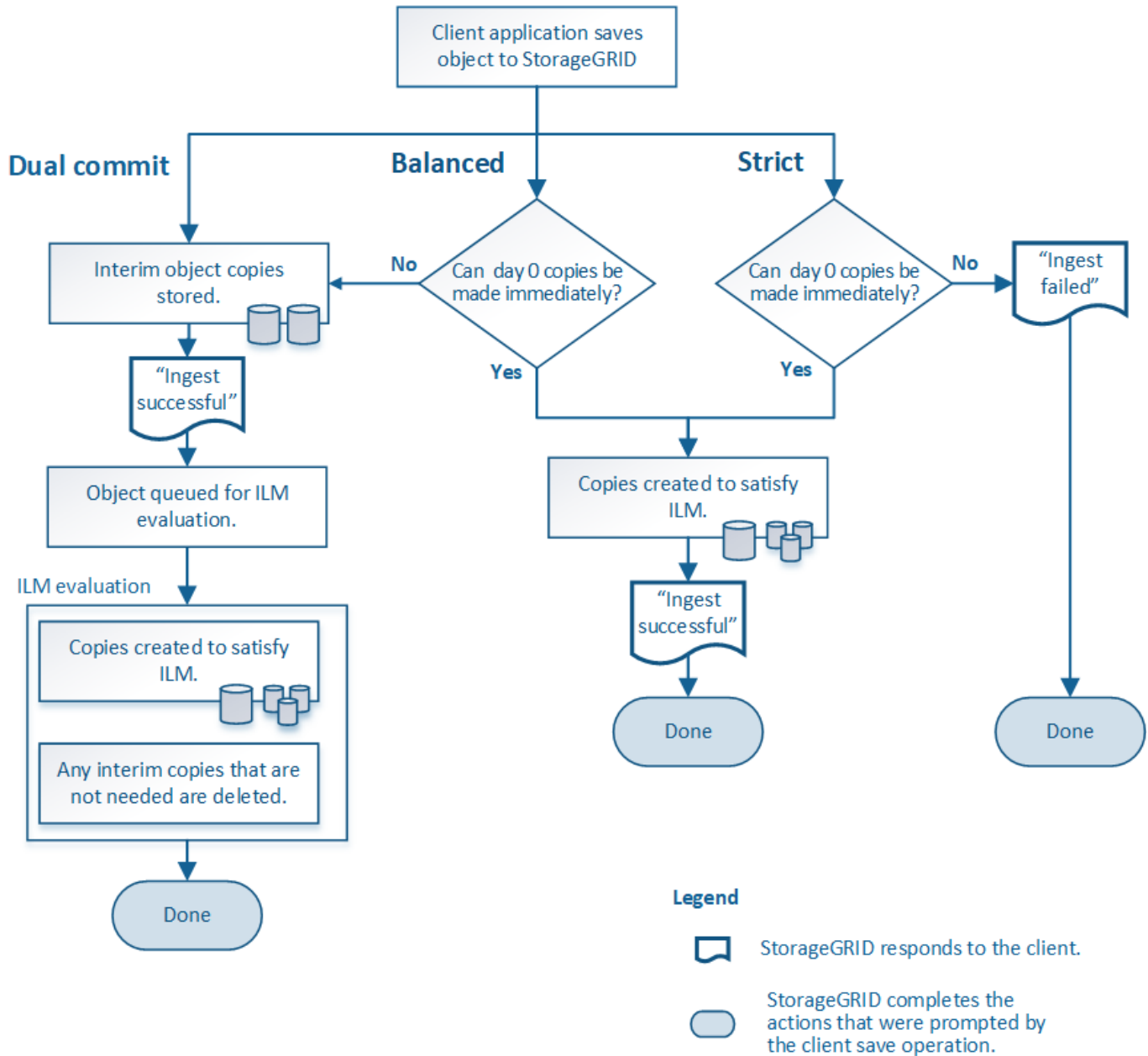
Lorsque vous créez une règle ILM, vous spécifiez l'une des trois options suivantes pour la protection des objets à leur entrée : double allocation, stricte ou équilibrée.

Selon votre choix, StorageGRID effectue des copies intermédiaires et met les objets en file d'attente pour

l'évaluation ILM. De plus, il utilise un placement synchrone et effectue immédiatement des copies pour répondre aux besoins de la solution ILM.

Organigramme des options d'ingestion

L'organigramme indique ce qui se passe lorsque les objets sont mis en correspondance par une règle ILM qui utilise chacune des trois options d'ingestion.



Double allocation

Lorsque vous sélectionnez l'option Dual Commit, StorageGRID réalise immédiatement des copies d'objet provisoires sur deux nœuds de stockage différents et renvoie un message d'« acquisition réussie » au client. L'objet est placé dans la file d'attente pour l'évaluation ILM et les copies correspondant aux instructions de placement de la règle sont créées ultérieurement. Si la règle ILM ne peut pas être traitée immédiatement après la double allocation, la protection contre la perte de site pourrait prendre du temps.

Utilisez l'option Dual commit dans l'un des cas suivants :

- Vous utilisez des règles ILM multisites et la latence d'ingestion du client est votre élément principal. Lorsque vous utilisez la fonctionnalité Dual Commit, vous devez vous assurer que votre grid peut effectuer le travail supplémentaire de création et de suppression des copies à double allocation si elles ne respectent pas la règle ILM. Détails :
 - La charge sur la grille doit être suffisamment faible pour éviter un backlog ILM.
 - La grille doit disposer de ressources matérielles excessives (IOPS, processeur, mémoire, bande passante réseau, etc.).
- Vous utilisez des règles ILM multisites et la connexion WAN entre les sites présente généralement une latence élevée ou une bande passante limitée. Dans ce scénario, l'utilisation de l'option de double engagement permet d'éviter les délais d'attente du client. Avant de choisir l'option Dual commit, il est recommandé de tester l'application cliente avec des charges de travail réalistes.

Équilibré (par défaut)

Lorsque vous sélectionnez l'option équilibrée, StorageGRID utilise également le placement synchrone lors de l'ingestion et immédiatement toutes les copies spécifiées dans les instructions de placement de la règle. Contrairement à l'option la plus stricte, si StorageGRID ne peut pas immédiatement effectuer toutes les copies, il utilise la fonction Dual commit. Si la politique ILM utilise des placements sur plusieurs sites et qu'il est impossible d'obtenir une protection immédiate contre la perte de site, l'alerte **ILM placement unatteignable** est déclenchée.

Utilisez l'option équilibrée afin de bénéficier de la meilleure combinaison possible de protection des données, de performances de grid et d'ingestion. Balanced est l'option par défaut de l'assistant de création de règles ILM.

Stricte

Lorsque vous sélectionnez une option stricte, StorageGRID utilise le placement synchrone pour l'ingestion et immédiatement toutes les copies d'objet spécifiées dans les instructions de placement de la règle. L'ingestion échoue si StorageGRID ne peut pas créer toutes les copies, par exemple, car l'emplacement de stockage requis est temporairement indisponible. Le client doit recommencer l'opération.

Utilisez l'option stricte si vous devez respecter des exigences opérationnelles ou réglementaires pour stocker immédiatement les objets aux emplacements définis dans la règle ILM. Par exemple, pour satisfaire aux exigences réglementaires, vous devrez peut-être utiliser l'option strict et un filtre avancé de contrainte d'emplacement pour garantir que les objets ne sont jamais stockés dans certains data centers.

Voir ["Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict"](#).

Avantages, inconvénients et limitations des options d'ingestion ILM dans StorageGRID

Découvrez les avantages et les inconvénients de chacune des trois options de protection des données à l'entrée (équilibre, stricte ou double engagement). Vous pouvez décider de la règle ILM à sélectionner.

Pour une vue d'ensemble des options d'acquisition, reportez-vous à la section ["Options d'ingestion"](#).

Avantages des options équilibrées et strictes

Par rapport à la double allocation qui crée des copies intermédiaires lors de l'ingestion, les deux options de placement synchrone offrent plusieurs avantages :

- **Meilleure sécurité des données:** Les données d'objet sont immédiatement protégées comme spécifié dans les instructions de placement de la règle ILM, qui peuvent être configurées de façon à protéger contre un large éventail de conditions de défaillance, y compris la défaillance de plusieurs emplacements de stockage. La double validation ne peut protéger que contre la perte d'une copie locale unique.
- *** Opération de grille plus efficace*:** Chaque objet est traité une seule fois, comme il est ingéré. Comme StorageGRID il n'est pas nécessaire de suivre ou de supprimer les copies intermédiaires, la charge de traitement est réduite et l'espace de base de données est consommé.
- **(équilibré) recommandé:** L'option équilibrée offre une efficacité ILM optimale. L'utilisation de l'option 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.
- *** (Strict) certitude sur les emplacements des objets*:** L'option stricte garantit que les objets sont immédiatement stockés conformément aux instructions de placement de la règle ILM.

Inconvénients des options équilibrées et strictes

Par rapport à Dual commit, les options équilibrées et strictes présentent quelques inconvénients :

- **Le client ingère plus longtemps:** Les latences d'entrée du client peuvent être plus longues. Lorsque vous utilisez les options équilibrées ou strictes, un message de « transfert réussi » n'est pas renvoyé au client tant que tous les fragments avec code d'effacement ou les copies répliquées ne sont pas créés et stockés. Néanmoins, les données d'objet atteindront leur placement final beaucoup plus vite.
- **(strict) taux plus élevés d'échec d'ingestion:** Avec l'option stricte, l'ingestion échoue lorsque StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle ILM. Si un emplacement de stockage requis est temporairement hors ligne ou si un problème réseau entraîne des retards dans la copie des objets entre les sites, des défaillances sont parfois à l'origine de taux élevés.
- **(strict) les parutions de téléchargement partitionné S3 peuvent ne pas être comme prévu dans certaines circonstances:** Avec strict, vous attendez que les objets soient placés comme décrit par la règle ILM ou pour que l'entrée échoue. Toutefois, avec un téléchargement partitionné S3, ILM est évalué pour chaque partie de l'objet lors de son ingestion, et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé. Dans les circonstances suivantes, cela peut entraîner des placements qui sont différents de ceux que vous attendez :
 - **Si le ILM change alors qu'un téléchargement partitionné S3 est en cours:** Parce que chaque pièce est placée conformément à la règle qui est active lors de l'ingestion de la pièce, certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement partitionné terminé. Dans ce cas, l'ingestion de l'objet n'a pas échoué. Toute pièce qui n'est pas correctement placée est placée dans la file d'attente pour une réévaluation ILM et sera déplacée ultérieurement à l'emplacement correct.
 - **Lorsque les règles ILM filtrent sur la taille :** lors de l'évaluation de ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évalué pour l'objet, toutes les parties de l'objet sont déplacées vers DC1.
- **(strict) l'ingestion n'échoue pas lorsque les balises d'objet ou les métadonnées sont mises à jour et les nouveaux placements ne peuvent pas être effectués :** avec stricte, les objets doivent être placés comme décrit par la règle ILM ou l'ingestion pour échouer. Toutefois, lorsque vous mettez à jour les métadonnées ou les balises d'un objet déjà stocké dans la grille, l'objet n'est pas réingéré. Cela signifie que toute modification du placement d'objet déclenchée par la mise à jour n'est pas effectuée immédiatement. Les changements de placement sont apportés lorsqu'ILM est réévaluée par des processus ILM en arrière-plan normaux. Si les modifications de positionnement requises ne peuvent pas

être effectuées (par exemple, parce qu'un nouvel emplacement requis n'est pas disponible), l'objet mis à jour conserve son positionnement actuel jusqu'à ce que les modifications de positionnement soient possibles.

Limitations sur les placements d'objets avec les options équilibrées et strictes

Les options équilibrées ou strictes ne peuvent pas être utilisées pour les règles ILM avec l'une des instructions de positionnement suivantes :

- Placement dans un pool de stockage cloud au premier jour.
- Placements 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, car StorageGRID ne peut pas effectuer de copies synchrones vers un pool de stockage cloud et une heure de création définie par l'utilisateur pourrait résoudre le problème actuel.

Impact des règles ILM et de la cohérence sur la protection des données

La règle ILM et la cohérence que vous choisissez affectent la protection des objets. 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 d'objet. Étant donné que StorageGRID requiert l'accès aux données et aux métadonnées d'un objet pour répondre aux demandes des clients, sélectionner des niveaux de protection correspondants pour assurer la cohérence et le comportement d'ingestion peut améliorer la protection initiale des données et fournir des réponses système plus prévisibles.

Voici un bref récapitulatif des valeurs de cohérence disponibles dans StorageGRID :

- **All** : tous les nœuds reçoivent immédiatement les métadonnées de l'objet ou la demande échoue.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites. Lorsque la sémantique du quorum est configurée, les comportements suivants s'appliquent :
 - Permet une tolérance aux pannes de site pour les demandes des clients lorsque les grilles comportent trois sites ou plus. Les réseaux à deux sites n'auront pas de tolérance aux pannes de site.
 - Les opérations S3 suivantes ne réussiront pas avec un site en panne :
 - DeleteBuckeEncryption
 - MettreBucketBranch
 - PutBucketEncryption
 - PutBuckeVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si nécessaire, vous pouvez ["configurer la sémantique du quorum StorageGRID pour une cohérence globale forte"](#) .

- **Strong-site** : les métadonnées de l'objet sont immédiatement distribuées à d'autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.

- **Read-After-New-write** : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.



Avant de sélectionner une valeur de cohérence, ["lisez la description complète de la cohérence"](#) . Vous devez comprendre les avantages et les limites avant de modifier la valeur par défaut.

Exemple de l'interaction des règles de cohérence et des règles ILM

Supposons que vous ayez une grille à trois sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez trois copies d'objet, une sur le site local et une sur chaque site distant. Adoptez un comportement d'ingestion strict.
- **Cohérence** : Forte-globale (les métadonnées de l'objet sont immédiatement distribuées sur plusieurs sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les trois copies de l'objet et distribue les métadonnées à plusieurs sites avant de renvoyer l'opération 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 les sites distants. L'objet est entièrement récupérable sur les autres sites.

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 les sites distants, 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'inter-relation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

["Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict"](#)

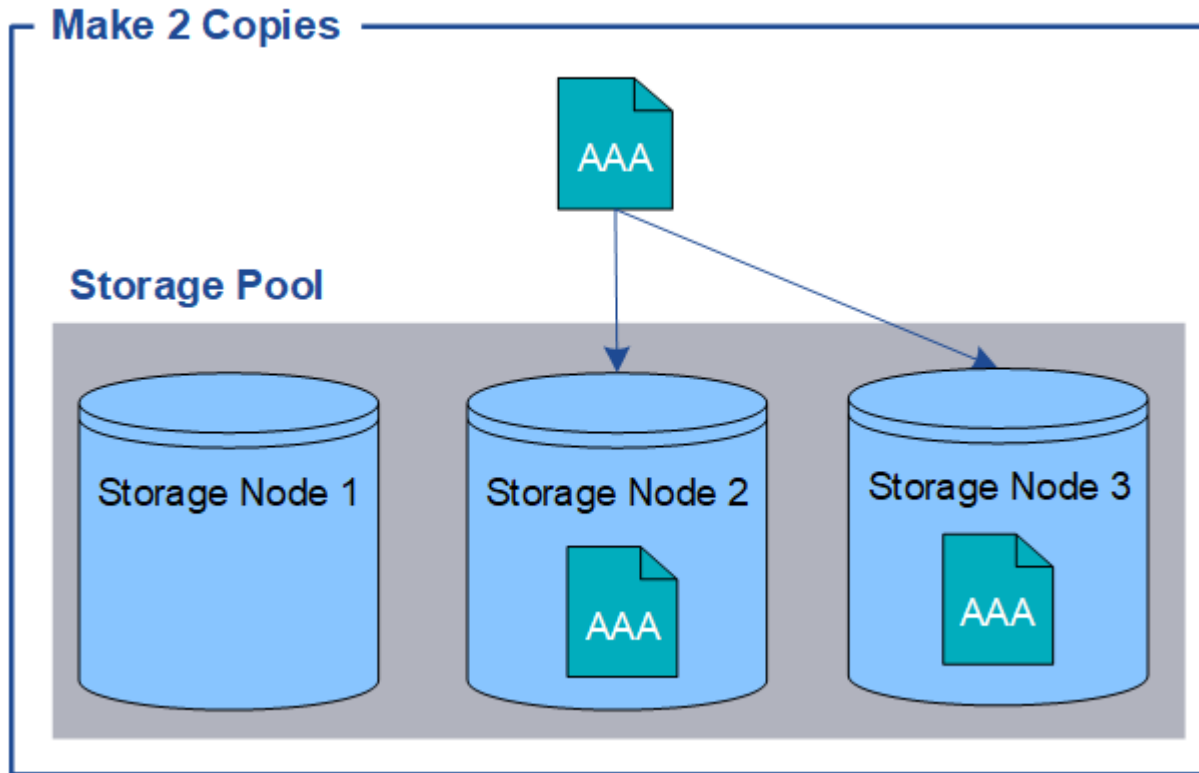
Le mode de stockage des objets (réplication ou code d'effacement)

Découvrez la réplication dans StorageGRID

La réplication est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objet (le code d'effacement est l'autre méthode). Lorsque les objets correspondent à une règle ILM utilisant la réplication, le système crée des copies exactes des données en mode objet et les stocke 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'emplacement où elles doivent être stockées, ainsi que la durée de stockage de ces copies à chaque emplacement.

L'exemple de règle ILM décrit deux copies répliquées de chaque objet placées dans un pool de stockage contenant trois nœuds de stockage.



Lorsque StorageGRID met les objets en correspondance avec cette règle, elle crée deux copies de l'objet, en plaçant chaque copie sur un autre nœud de stockage du pool. Les deux copies peuvent être placées sur deux des trois nœuds de stockage disponibles. Dans ce cas, la règle a placé des copies d'objet sur les nœuds de stockage 2 et 3. Comme il existe deux copies, l'objet peut être récupéré en cas de défaillance de l'un des nœuds du pool de stockage.



StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si le grid inclut trois nœuds de stockage et que vous créez une règle ILM de 4 copies, seules trois copies sont effectuées, une copie pour chaque nœud de stockage. L'alerte **ILM placement inaccessible** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Informations associées

- ["Qu'est-ce que le code d'effacement"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Protection contre la perte de site à l'aide de la réplication et du code d'effacement"](#)

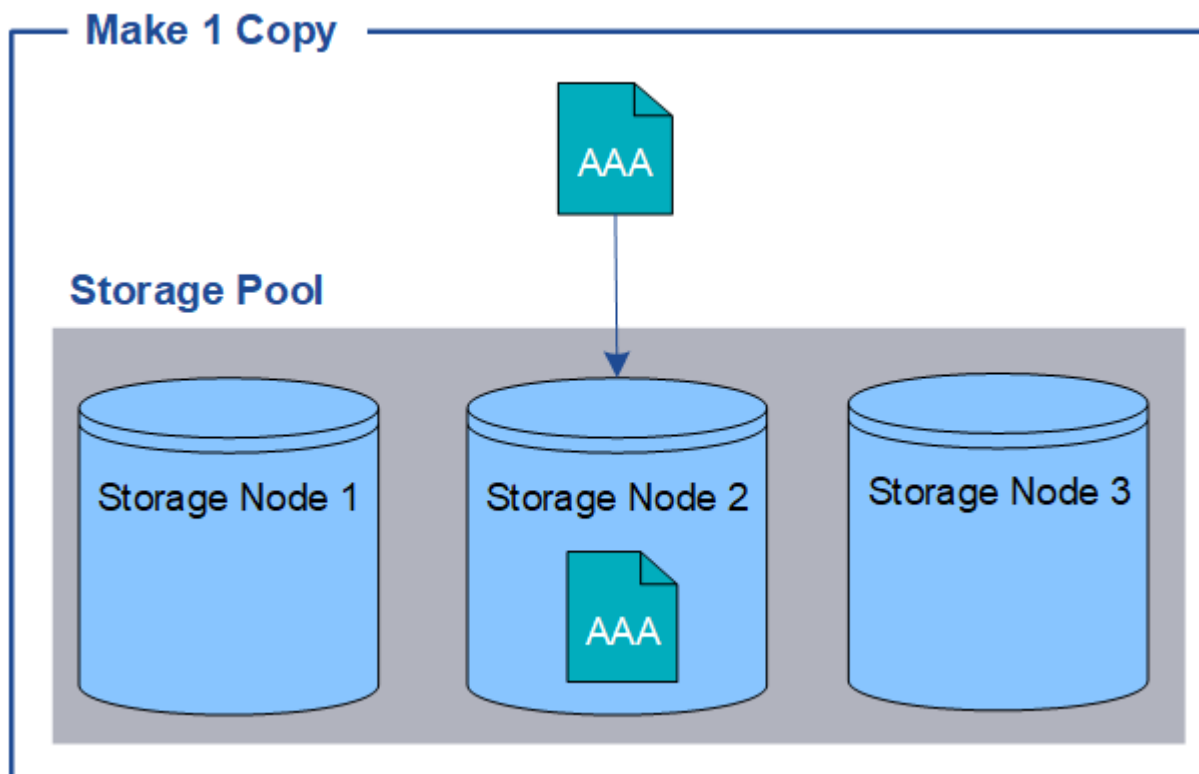
Risques de la réplication à copie unique dans StorageGRID

Lors de la création d'une règle ILM pour créer des copies répliquées, vous devez toujours spécifier au moins deux copies pour une période donnée dans les instructions de placement.



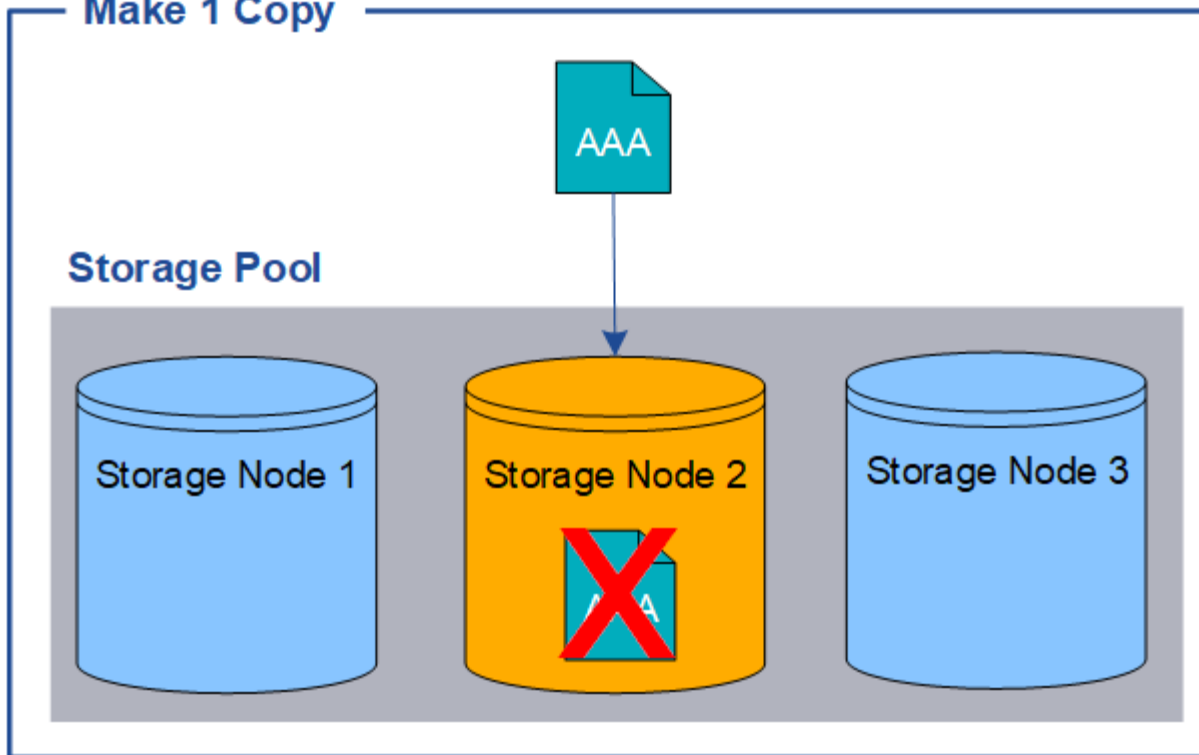
N'utilisez pas de règle ILM pour créer une seule copie répliquée pour une période donnée. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Dans l'exemple suivant, la règle ILM Make 1 copie spécifie qu'une copie répliquée d'un objet doit être placée dans un pool de stockage contenant trois nœuds de stockage. Lors de l'ingestion d'un objet qui correspond à cette règle, StorageGRID place une copie unique sur un seul nœud de stockage.

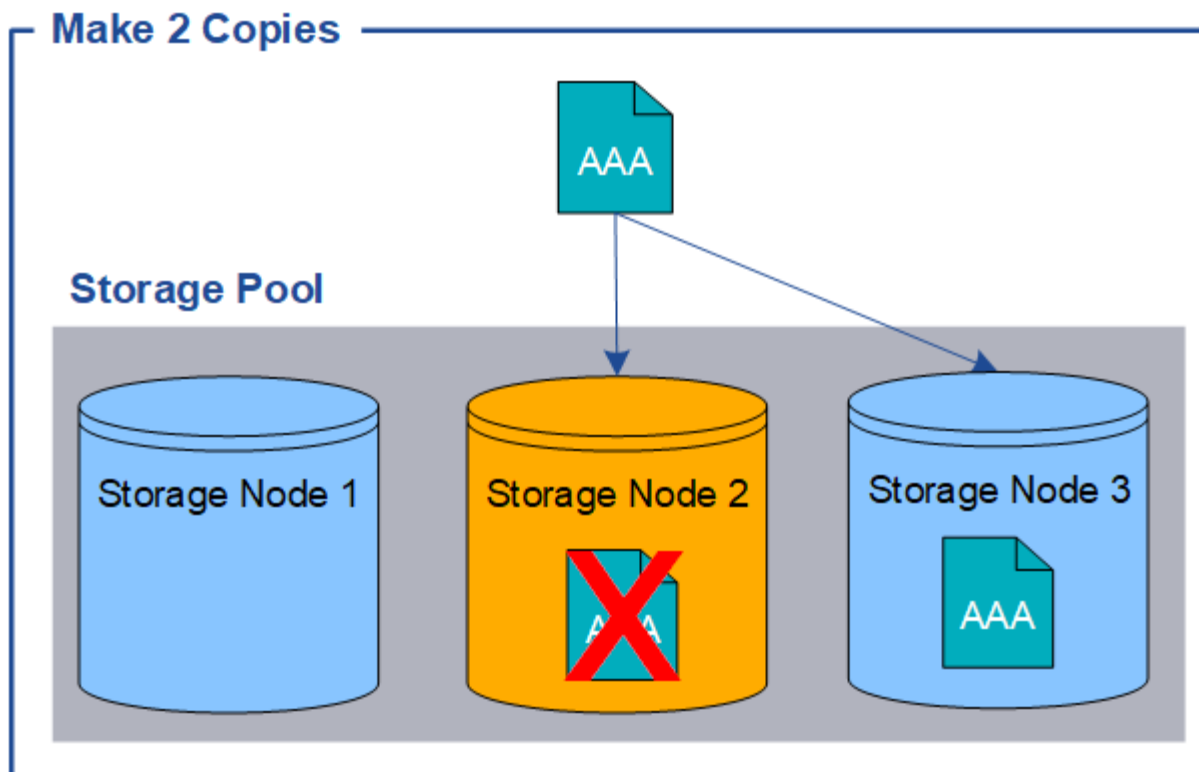


Lorsqu'une règle ILM ne crée qu'une seule copie répliquée d'un objet, cet objet devient inaccessible lorsque le nœud de stockage est indisponible. Dans cet exemple, vous perdrez temporairement l'accès à l'objet AAA chaque fois que le nœud de stockage 2 est hors ligne, par exemple lors d'une procédure de mise à niveau ou de maintenance. Vous perdrez entièrement l'objet AAA en cas de défaillance du nœud de stockage 2.

Make 1 Copy



Pour éviter de perdre des données d'objet, vous devez toujours effectuer au moins deux copies de tous les objets à protéger par la réplication. Si deux copies ou plus existent, vous pouvez toujours accéder à l'objet en cas de panne ou de mise hors ligne d'un nœud de stockage.



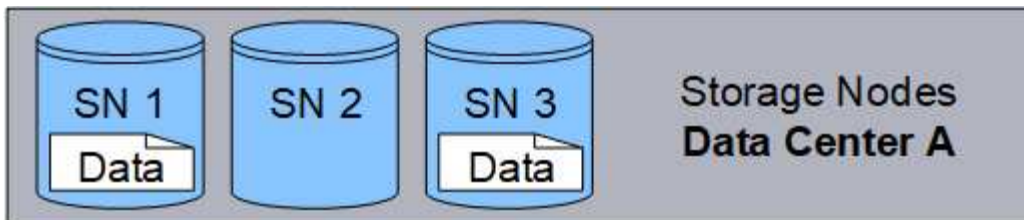
Découvrez le code d'effacement dans StorageGRID

Le code d'effacement fait partie des deux méthodes utilisées par StorageGRID pour stocker les données en mode objet (la réplication est l'autre méthode). Lorsque les objets correspondent à une règle ILM utilisant le code d'effacement, ces objets sont découpés en fragments de données, des fragments de parité supplémentaires sont calculés et chaque fragment est stocké sur un autre nœud de stockage.

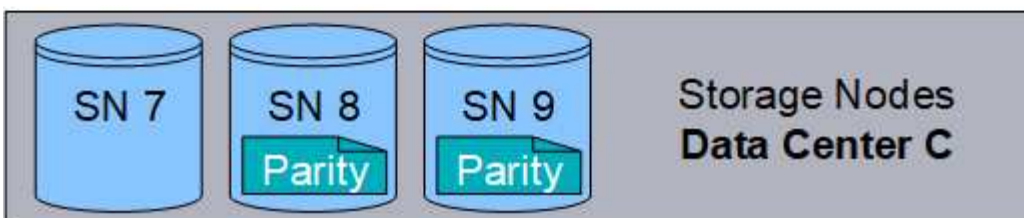
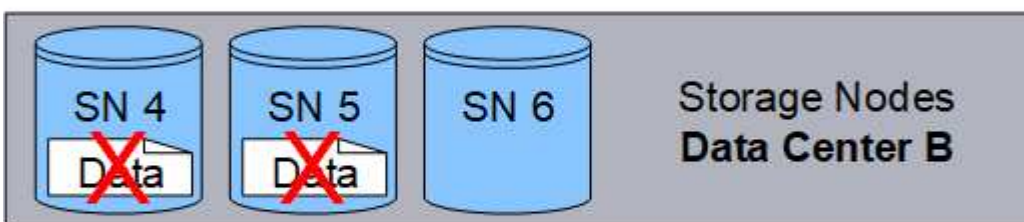
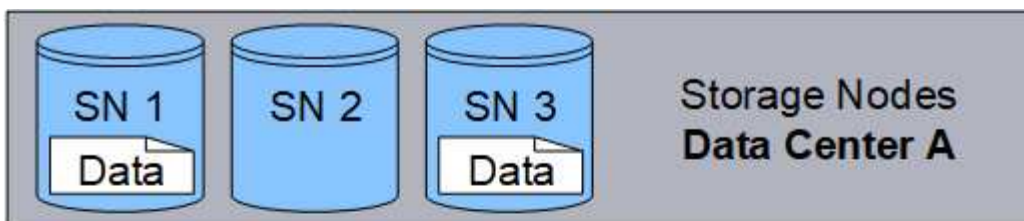
Lorsqu'un objet est accédé, il est réassemblé à l'aide des fragments stockés. En cas de corruption ou de perte d'un fragment de parité, l'algorithme de code d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des données restantes et des fragments de parité.

Au fur et à mesure que vous créez des règles ILM, StorageGRID crée des profils de code d'effacement qui prennent en charge ces règles. Vous pouvez afficher la liste des profils de code d'effacement, [renommer un profil de code d'effacement](#), ou [Désactivez un profil de code d'effacement s'il n'est actuellement utilisé dans aucune règle ILM](#).

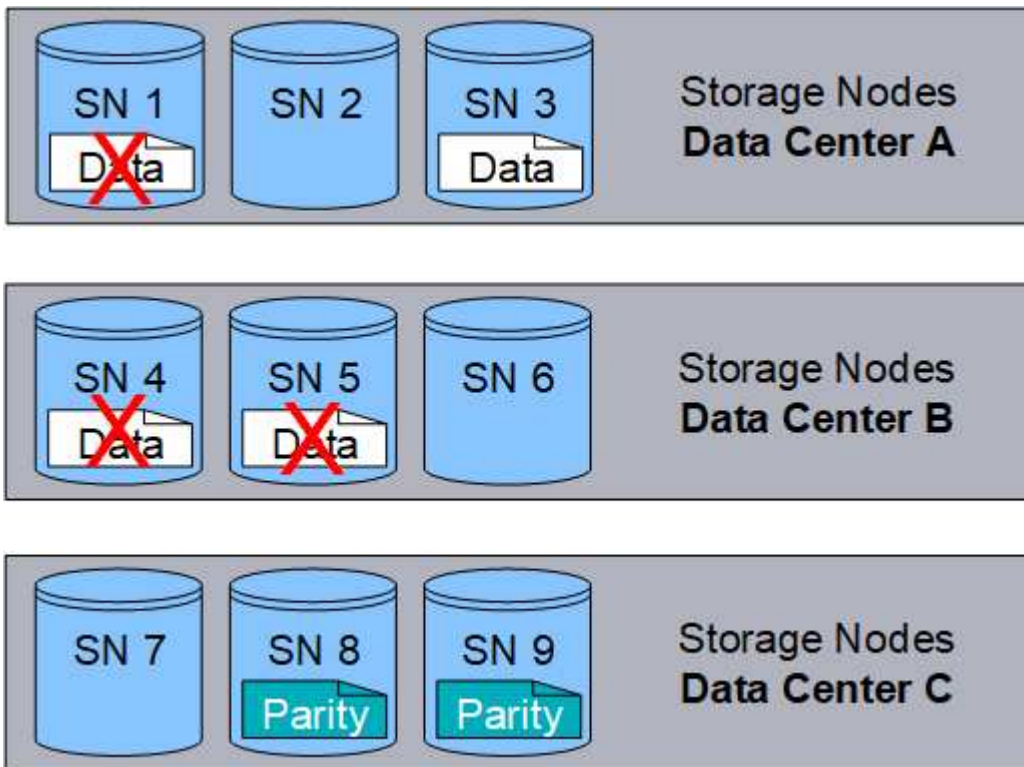
L'exemple suivant illustre l'utilisation d'un algorithme de code d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de code d'effacement 4+2. Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données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



Le schéma de code d'effacement 4+2 peut être configuré de différentes manières. Par exemple, vous pouvez configurer un pool de stockage sur un seul site qui contient six nœuds de stockage. Pour "[protection contre la perte de site](#)", vous pouvez utiliser un pool de stockage contenant trois sites avec trois nœuds de stockage sur chaque site. Un objet peut être récupéré tant que quatre des six fragments (données ou parité) restent disponibles. Jusqu'à deux fragments peuvent être perdus sans perte des données de l'objet. Si un site entier est perdu, l'objet peut toujours être récupéré ou réparé, tant que tous les autres fragments restent accessibles.



Si plus de deux nœuds de stockage sont perdus, l'objet n'est pas récupérable.



Informations associées

- ["Qu'est-ce que la réplication"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Que sont les schémas de code d'effacement"](#)
- ["Renommer un profil de code d'effacement"](#)
- ["Désactiver un profil de code d'effacement"](#)

Découvrez les schémas de code d'effacement dans StorageGRID

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 code d'effacement disponible. StorageGRID crée automatiquement des schémas de code d'effacement en fonction du nombre de nœuds et de sites qui composent le pool de stockage que vous souhaitez utiliser.

Protection des données

Le système StorageGRID utilise l'algorithme de codage d'effacement Reed-Solomon. L'algorithme coupe un objet en k fragments de données et calcule les m fragments de parité.

Les $k + m = n$ fragments sont répartis entre les 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 des m fragments perdus ou corrompus. Plus la valeur de m est élevée, plus la tolérance de panne est élevée.

La meilleure protection des données est assurée par le schéma de code d'effacement avec la tolérance de défaillance de nœud ou de volume la plus élevée au sein d'un pool de stockage.

Surcharge du stockage

La surcharge de stockage d'un schéma de code d'effacement est calculée en divisant le nombre de fragments de parité (m) par le nombre de fragments de données (k). Vous pouvez utiliser la surconsommation de stockage pour calculer la quantité d'espace disque requise par chaque objet avec code d'effacement :

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Par exemple, si vous stockez un objet de 10 Mo avec le schéma 4+2 (qui affiche une surcharge du stockage de 50 %), l'objet utilise 15 Mo de stockage grid. Si vous stockez le même objet de 10 Mo avec le schéma 6+2 (qui affiche une surcharge de stockage de 33 %), l'objet consomme environ 13.3 Mo.

Sélectionnez le schéma de code d'effacement dont la valeur totale est la plus faible, en fonction de $k+m$ vos besoins. Les schémas de code d'effacement avec un nombre réduit de fragments sont plus efficaces sur le plan de la capacité de calcul car :

- Un nombre inférieur de fragments est créé et distribué (ou récupéré) par objet
- Elles offrent de meilleures performances car la taille de fragment est plus grande
- En outre, moins de nœuds peuvent être ajoutés dans un ["l'extension des systèmes permet de stocker plus de stockage"](#)

Instructions relatives aux pools de stockage

Lorsque vous sélectionnez le pool de stockage à utiliser pour une règle qui crée une copie avec code d'effacement, suivez les consignes suivantes pour les pools de stockage :

- Le pool de stockage doit inclure trois sites ou plus, ou exactement un site.



Le code d'effacement ne peut pas être utilisé si le pool de stockage comprend deux sites.

- [Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites](#)
- [Schémas de code d'effacement pour pools de stockage sur un site](#)
- N'utilisez pas de pool de stockage incluant le site tous les sites.
- Le pool de stockage doit inclure au moins les $k+m + 1$ nœuds de stockage capables de stocker les données d'objet.



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir des données et des métadonnées d'objet (nœud de stockage « combiné »), uniquement des métadonnées d'objet ou uniquement des données d'objet. Pour plus d'informations, reportez-vous à ["Types de nœuds de stockage"](#) .

Le nombre minimal de nœuds de stockage requis est $k+m$. Toutefois, il est possible de disposer d'au moins un nœud de stockage supplémentaire pour empêcher les défaillances d'entrée et les arriérés ILM en cas d'indisponibilité temporaire d'un nœud de stockage requis.

Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites

Le tableau ci-dessous décrit les schémas de code d'effacement actuellement pris en charge par StorageGRID pour les pools de stockage incluant au moins trois sites. Tous ces programmes offrent une protection contre les pertes de site. Un site peut être perdu et l'objet sera toujours accessible.

Pour les schémas de code d'effacement qui assurent une protection contre la perte de site, le nombre recommandé de nœuds de stockage dans le pool de stockage dépasse $k+m + 1$ car chaque site requiert au moins trois nœuds de stockage.

Schéma de code d'effacement ($k+m$)	Nombre minimal de sites déployés	Nombre recommandé de nœuds de stockage sur chaque site	Nombre total recommandé de nœuds de stockage	Protection contre la perte de site ?	Surcharge du stockage
4+2	3	3	9	Oui	50%
6+2	4	3	12	Oui	33%
8+2	5	3	15	Oui	25%
6+3	3	4	12	Oui	50%
9+3	4	4	16	Oui	33%
2+1	3	3	9	Oui	50%
4+1	5	3	15	Oui	25%
6+1	7	3	21	Oui	17%
7+5	3	5	15	Oui	71%



StorageGRID requiert au moins trois nœuds de stockage par site. Pour utiliser le schéma 7+5, chaque site requiert au moins quatre nœuds de stockage. Il est recommandé d'utiliser cinq nœuds de stockage par site.

Lors de la sélection d'un schéma de code d'effacement assurant la protection du site, équilibrez l'importance relative des facteurs suivants :

- **Nombre de fragments:** La performance et la flexibilité d'expansion sont généralement meilleures quand le nombre total de fragments est plus faible.
- **Tolérance aux pannes :** la tolérance aux pannes est augmentée en ayant plus de segments de parité (c'est-à-dire lorsque m a une valeur plus élevée).
- **Trafic réseau:** Lors de la récupération après des pannes, l'utilisation d'un schéma avec plus de fragments (c'est-à-dire, un total plus élevé pour $k+m$) crée plus de trafic réseau.
- **Surcharge de stockage :** les schémas qui génèrent une surcharge plus élevée requièrent davantage d'espace de stockage par objet.

Par exemple, lorsque vous décidez d'un schéma 4+2 et 6+3 (qui ont tous deux des frais de stockage de 50 %), sélectionnez le schéma 6+3 si une tolérance de panne supplémentaire est nécessaire. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées. Si tous les autres facteurs sont égaux, sélectionnez 4+2 parce qu'il a un nombre total de fragments inférieur.



Si vous n'êtes pas certain du schéma à utiliser, sélectionnez 4+2 ou 6+3, ou contactez le support technique.

Schémas de code d’effacement pour pools de stockage sur un site

Un pool de stockage sur un site prend en charge tous les schémas de codage d’effacement définis pour trois sites ou plus, à condition que le site dispose de suffisamment de nœuds de stockage.

Le nombre minimal de nœuds de stockage requis est $k+m$, mais un pool de stockage avec des $k+m + 1$ nœuds de stockage est recommandé. Par exemple, le schéma de code d’effacement 2+1 requiert un pool de stockage avec au moins trois nœuds de stockage, mais quatre nœuds de stockage sont recommandés.

Schéma de code d’effacement ($k+m$)	Nombre minimal de nœuds de stockage	Nombre recommandé de nœuds de stockage	Surcharge du stockage
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Avantages, inconvénients et exigences du code d’effacement dans StorageGRID

Avant de décider s’il est nécessaire d’utiliser la réplication ou le codage d’effacement pour protéger les données d’objet contre la perte, vous devez connaître les avantages, les inconvénients et les exigences du codage d’effacement.

Avantages du code d’effacement

Par rapport à la réplication, le codage d’effacement assure une fiabilité, une disponibilité et une efficacité du stockage supérieures.

- **Fiabilité** : Mesurée par le nombre de pannes simultanées pouvant être subies sans perte de données.
 - Réplication : plusieurs copies d'objets identiques sont stockées sur différents nœuds et sur plusieurs sites.
 - 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.
- **Disponibilité** : La possibilité d'obtenir 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 une disponibilité et une fiabilité similaires, les objets codés par effacement utilisent moins d'espace disque que les objets répliqués. 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 des objets avec code d'effacement est calculé selon la taille de l'objet et la surcharge du stockage. Le pourcentage de surcharge de stockage est le nombre de fragments de parité divisé par le nombre de fragments de données.

Inconvénients du code d'effacement

Par rapport à la réplication, le code d'effacement présente les inconvénients suivants :

- En fonction du schéma de code d'effacement, une augmentation du nombre de nœuds et de sites de stockage est recommandée. En revanche, si vous répliquez les données d'objet, vous n'avez besoin que d'un seul nœud de stockage pour chaque copie. Voir ["Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites"](#) et ["Schémas de code d'effacement pour pools de stockage sur un site"](#).
- Coût et complexité accrus de l'expansion du stockage. Pour étendre un déploiement qui utilise la réplication, vous ajoutez de la capacité de stockage à chaque emplacement où les copies d'objet sont effectuées. Pour étendre un déploiement qui utilise le code d'effacement, vous devez tenir compte à la fois du schéma de code d'effacement utilisé et de la façon dont les nœuds de stockage existants sont complets. Par exemple, si vous attendez que les nœuds existants soient pleins à 100 %, vous devez ajouter au moins $k+m$ nœuds de stockage. Toutefois, si vous développez lorsque les nœuds existants sont pleins à 70 %, vous pouvez ajouter deux nœuds par site tout en optimisant la capacité de stockage utilisable. Pour plus d'informations, voir ["Ajoutez de la capacité de stockage pour les objets avec code d'effacement"](#).
- Le codage d'effacement entre sites répartis géographiquement augmente la latence de récupération. Les fragments d'objet d'un objet dont le code d'effacement et la distribution sont répartis sur des sites distants sont plus longs à récupérer sur des connexions WAN qu'un objet répliqué et disponible localement (le site auquel le client se connecte).
- Lorsque vous utilisez le codage d'effacement sur des sites répartis géographiquement, le trafic réseau WAN est plus important pour les récupérations et les réparations, en particulier pour les objets fréquemment récupérés ou pour la réparation d'objets via les connexions réseau WAN.
- Lorsque vous utilisez le codage d'effacement sur plusieurs sites, le débit maximal des objets diminue fortement à mesure que la latence du réseau entre les sites augmente. Cette diminution est le résultat d'une diminution du débit du réseau TCP, ce qui affecte la rapidité avec laquelle le système StorageGRID peut stocker et récupérer des fragments d'objet.
- Plus grande utilisation des ressources de calcul.

Quand utiliser le code d'effacement

Utilisez le codage d'effacement pour les exigences suivantes :

- Objets dont la taille est supérieure à 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

- Stockage à long terme ou à froid pour le contenu rarement récupéré.
- Haute disponibilité et fiabilité des données.
- Protégez-vous contre les défaillances complètes du site et des nœuds.
- Efficacité du stockage.
- Les déploiements sur un seul site exigent une protection efficace des données avec une seule copie avec code d'effacement plutôt que plusieurs copies répliquées.
- Déploiements sur plusieurs sites pour lesquels la latence inter-site est inférieure à 100 ms.

Comment StorageGRID détermine la conservation des objets

StorageGRID fournit aux administrateurs du grid et aux utilisateurs de locataires individuels les options permettant de spécifier la durée de stockage des objets. En général, les instructions de conservation fournies par un utilisateur locataire ont priorité sur les instructions de conservation fournies par l'administrateur de la grille.

Contrôle de la conservation des objets par les utilisateurs locataires

Les utilisateurs locataires peuvent utiliser ces méthodes pour contrôler la durée de stockage de leurs objets dans StorageGRID :

- Si le paramètre global S3 Object Lock est activé pour la grille, les utilisateurs locataires S3 peuvent créer des compartiments avec S3 Object Lock activé, puis sélectionner une **période de conservation par défaut** pour chaque compartiment.
- Si le paramètre global S3 Object Lock est activé pour la grille, les locataires S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation à la date et la conservation légale de chaque version d'objet ajoutée dans ce compartiment.
 - Aucune méthode ne permet de supprimer une version d'objet faisant l'objet d'une conservation légale.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut pas être supprimée par aucune méthode.
 - Les objets d'un compartiment lorsque le verrouillage d'objet S3 est activé sont conservés « indéfiniment » par ILM. Une fois la date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou l'expiration du cycle de vie du compartiment. Voir ["Gestion des objets avec le verrouillage d'objets S3"](#).
- Les locataires S3 peuvent ajouter une configuration du cycle de vie à leurs compartiments pour définir une action d'expiration. En cas de cycle de vie d'un compartiment, StorageGRID stocke un objet jusqu'à ce que la date ou le nombre de jours spécifiés dans l'action expiration soit atteint, à moins que le client ne supprime d'abord l'objet. Voir ["Création de la configuration du cycle de vie S3"](#).

- Un client S3 peut émettre une demande de suppression d'objet. StorageGRID privilégie toujours les demandes de suppression client sur le cycle de vie du compartiment S3 ou la ILM pour déterminer si supprimer ou conserver un objet.

Comment les administrateurs du grid contrôlent-ils la conservation des objets

Les administrateurs du grid peuvent utiliser ces méthodes pour contrôler la conservation des objets :

- Définissez une période de conservation maximale du verrouillage objet S3 pour chaque locataire. Les utilisateurs locataires peuvent ensuite définir une période de conservation par défaut pour chacun de leurs compartiments. La période de conservation maximale est également appliquée aux objets nouvellement ingérés pour ce compartiment (date de conservation jusqu'à l'objet).
- Créez des instructions de placement ILM pour contrôler la durée de stockage des objets. Lorsque les objets sont comparés par une règle ILM, StorageGRID les stocke jusqu'à la dernière période de la règle ILM. Les objets sont conservés indéfiniment si « indéfiniment » est spécifié pour les instructions de placement.
- Indépendamment de la durée de conservation des objets, les paramètres ILM contrôlent les types de copies d'objet (répliquées ou codées d'effacement) stockées et l'emplacement de ces copies (nœuds de stockage ou pools de stockage cloud).

Interaction du cycle de vie des compartiments S3 et de la ILM

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

Exemples de conservation d'objets

Pour mieux comprendre les interactions entre le verrouillage objet S3, les paramètres du cycle de vie des compartiments, les demandes de suppression de clients et la gestion des règles ILM, prenez en compte ces exemples.

Exemple 1 : le cycle de vie des compartiments S3 permet de conserver les objets plus longtemps que ILM

ILM

Stockez deux copies pendant 1 an (365 jours)

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Résultat

StorageGRID stocke l'objet pendant 730 jours. StorageGRID utilise les paramètres du cycle de vie du compartiment pour déterminer s'il faut supprimer ou conserver un objet.



Si le cycle de vie des compartiments précise que les objets doivent être conservés plus longtemps que spécifié par l'ILM, StorageGRID continue d'utiliser les instructions de placement du ILM pour déterminer le nombre et le type de copies à stocker. Dans cet exemple, deux copies de l'objet continueront à être stockées dans StorageGRID au lieu de 366 à 730 jours.

Exemple 2 : le cycle de vie des compartiments S3 expire les objets avant la gestion du cycle de vie des règles

ILM

Stockage de deux copies pendant 2 ans (730 jours)

Cycle de vie des compartiments

Expiration des objets en 1 an (365 jours)

Résultat

StorageGRID supprime les deux copies de l'objet après le jour 365.

Exemple 3 : la suppression du client annule le cycle de vie du compartiment et la ILM

ILM

Stockage de deux copies sur des nœuds de stockage « à l'infini »

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Demande de suppression du client

Émis le jour 400

Résultat

StorageGRID supprime les deux copies de l'objet le jour 400 en réponse à la requête de suppression du client.

Exemple 4 : le verrouillage d'objet S3 remplace la demande de suppression du client

Verrouillage d'objet S3

Conserver jusqu'à ce jour pour une version d'objet : 2026-03-31. Une obligation légale n'est pas en vigueur.

Règle ILM conforme

Stockage de deux copies sur des nœuds de stockage « à l'infini »

Demande de suppression du client

Publiée le 2024-03-31

Résultat

StorageGRID ne supprimera pas la version de l'objet car la date de conservation est encore à 2 ans.

Comment StorageGRID supprime des objets

StorageGRID peut supprimer des objets en réponse directe à une requête d'un client ou automatiquement à la suite de l'expiration du cycle de vie d'un compartiment S3 ou des exigences de la politique ILM. Pour gérer plus efficacement les objets, il est important de comprendre les différentes méthodes de suppression des objets et la façon dont StorageGRID les gère.

StorageGRID peut utiliser l'une des deux méthodes suivantes pour supprimer les objets :

- **Suppression synchrone** : lorsque StorageGRID reçoit une demande de suppression de client, toutes les copies d'objet sont supprimées immédiatement. Le client est informé que la suppression a réussi une fois les copies supprimées.
- **Les objets sont placés en file d'attente pour suppression** : lorsque StorageGRID reçoit une requête de suppression, l'objet est mis en attente pour suppression et le client est immédiatement informé de l'réussie de cette suppression. Les copies d'objet sont supprimées ultérieurement par le traitement ILM en arrière-plan.

Lors de la suppression d'objets, StorageGRID utilise la méthode qui optimise les performances de suppression, réduit les retards de suppression et libère de l'espace le plus rapidement possible.

Le tableau résume le moment où StorageGRID utilise chaque méthode.

Méthode d'exécution de la suppression	Lorsqu'il est utilisé
Les objets sont placés en file d'attente pour suppression	Lorsque l'une des conditions suivantes est vraie : • La suppression automatique d'objet a été déclenchée par l'un des événements suivants : ◦ La date d'expiration ou le nombre de jours pendant la configuration du cycle de vie d'un compartiment S3 est atteint. ◦ La dernière période spécifiée dans une règle ILM s'écoule. Remarque : les objets d'un compartiment pour lequel le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont en attente légale ou si une date de conservation jusqu'à a été spécifiée mais pas encore remplie. • Un client S3 demande la suppression et une ou plusieurs des conditions suivantes sont remplies : ◦ Les copies ne peuvent pas être supprimées dans les 30 secondes qui suivent, car, par exemple, un emplacement d'objet est temporairement indisponible. ◦ Les files d'attente de suppression d'arrière-plan sont inactives.
Suppression immédiate d'objets (suppression synchrone)	Lorsqu'un client S3 effectue une requête de suppression et que toutes des conditions suivantes sont remplies : • Toutes les copies peuvent être supprimées en 30 secondes. • Les files d'attente de suppression d'arrière-plan contiennent des objets à traiter.

Lorsque les clients S3 font des demandes de suppression, StorageGRID commence par ajouter des objets à la file d'attente de suppression. Il passe ensuite en mode suppression synchrone. S'assurer que la file d'attente de suppression en arrière-plan contient des objets à traiter, ce qui permet à StorageGRID de traiter les suppressions plus efficacement, en particulier pour les clients à faible simultanéité, tout en aidant à empêcher la suppression des arriérés du client.

Temps nécessaire à la suppression des objets

La façon dont StorageGRID supprime des objets peut avoir un impact sur le fonctionnement du système :

- Lorsque StorageGRID effectue une suppression synchrone, StorageGRID peut donner jusqu'à 30 secondes pour renvoyer un résultat au client. Cela signifie que la suppression peut se produire plus lentement, même si les copies sont réellement supprimées plus rapidement que lors de la mise en file d'attente d'objets StorageGRID pour suppression.
- Si vous surveillez de près les performances de suppression lors d'une suppression en bloc, vous remarquerez peut-être que la vitesse de suppression semble lente après la suppression d'un certain nombre d'objets. Ce changement survient lorsque StorageGRID passe d'objets de mise en file d'attente pour suppression à des fins de suppression synchrone. La réduction apparente du taux de suppression ne signifie pas que les copies d'objet sont supprimées plus lentement. Au contraire, elle indique qu'en moyenne, l'espace est maintenant libéré plus rapidement.

Si vous supprimez un grand nombre d'objets et que vous souhaitez libérer rapidement de l'espace, pensez à utiliser une requête client pour supprimer des objets au lieu de les supprimer à l'aide d'ILM ou d'autres méthodes. En général, l'espace est libéré plus rapidement lors de la suppression d'espace par les clients, car StorageGRID peut utiliser la suppression synchrone.

Le temps nécessaire pour libérer de l'espace après la suppression d'un objet dépend de plusieurs facteurs :

- Si les copies d'objet sont supprimées de manière synchrone ou mises en file d'attente pour être supprimées ultérieurement (pour les demandes de suppression de client).
- D'autres facteurs, tels que le nombre d'objets dans la grille ou la disponibilité des ressources de la grille lorsque les copies d'objet sont mises en file d'attente pour suppression (pour les suppressions de clients et d'autres méthodes).

Suppression d'objets avec version S3

Lorsque le contrôle de version est activé pour un compartiment S3, StorageGRID suit un comportement Amazon S3 pour répondre aux demandes de suppression, qu'elles proviennent d'un client S3, de l'expiration d'un cycle de vie d'un compartiment S3 ou des exigences de la règle ILM.

Lorsque des objets sont versionnés, les demandes de suppression d'objets ne suppriment pas la version actuelle de l'objet et ne libèrent pas d'espace. Une demande de suppression d'objet crée un marqueur de suppression de zéro octet en tant que 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 courante.

Bien que l'objet n'ait pas été supprimé, StorageGRID se comporte comme si la version actuelle de l'objet n'est plus disponible. Les requêtes à cet objet renvoient 404 Not Found. Cependant, les données d'objet non actuelles n'ayant pas été supprimées, les demandes qui spécifient une version non actuelle de l'objet peuvent réussir.

Si un client supprime une version d'objet avec un ID de version d'un [seau de branche](#) StorageGRID masque l'existence de la version de l'objet mais ne crée pas de marqueur de suppression dans le bucket de branche. Si un client supprime un objet sans ID de version d'un bucket de branche, StorageGRID crée un marqueur de suppression dans le bucket de branche conformément au comportement S3 standard.

Pour libérer de l'espace lors de la suppression d'objets multiversion ou pour supprimer des marqueurs de suppression, utilisez l'une des méthodes suivantes :

- **Demande client S3** : spécifiez l'ID de version de l'objet dans la demande de SUPPRESSION D'objet S3

(DELETE /object?versionId=ID). Notez que cette demande ne supprime que les copies d'objet pour la version spécifiée (les autres versions occupent toujours de l'espace).

- **Cycle de vie du compartiment** : utilisez l'`NoncurrentVersionExpiration` action dans la configuration du cycle de vie du compartiment. Lorsque le nombre de NoncurrentDays spécifié est atteint, StorageGRID supprime définitivement toutes les copies des versions d'objets non courants. Ces versions d'objet ne peuvent pas être restaurées.

L'`NewerNoncurrentVersions` action dans la configuration du cycle de vie du compartiment spécifie le nombre de versions non actuelles conservées dans un compartiment S3 versionné. S'il y a plus de versions non actuelles que `NewerNoncurrentVersions` ce qui est spécifié, StorageGRID supprime les versions plus anciennes lorsque la valeur NoncurrentDays s'est écoulée. Le `NewerNoncurrentVersions` seuil remplace les règles de cycle de vie fournies par ILM, ce qui signifie qu'un objet non courant avec une version comprise dans le seuil est conservé si une `NewerNoncurrentVersions` ILM demande sa suppression.

Pour supprimer les marqueurs de suppression d'objets expirés, utilisez `Expiration` l'action avec l'une des balises suivantes : `ExpiredObjectDeleteMarker`, `Days` ou `Date`.

- **ILM: "Cloner une règle active"** Et ajouter deux règles ILM à la nouvelle politique:
 - Première règle : utilisez « Noncurrent Time » comme heure de référence pour faire correspondre les versions non actuelles de l'objet. Dans "[Étape 1 \(entrer les détails\) de l'assistant de création de règles ILM](#)", sélectionnez **Oui** pour la question, "appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée) ?"
 - Deuxième règle : utilisez **le temps d'ingestion** pour correspondre à la version actuelle. La règle « Noncurrent Time » doit apparaître dans la police au-dessus de la règle **Ingest Time**.

Pour supprimer les marqueurs de suppression d'objets expirés, utilisez une règle **heure de réception** pour correspondre aux marqueurs de suppression actuels. Les marqueurs de suppression ne sont supprimés que lorsqu'une **période de jours** est passée et que le créateur de suppression actuel est arrivé à expiration (il n'y a pas de versions non actuelles).

- **Supprimer les objets dans le compartiment** : utilisez le gestionnaire de tenant pour "[supprimez toutes les versions d'objet](#)", y compris les marqueurs de suppression, à partir d'un compartiment.

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 les marqueurs de suppression doivent être supprimés avant qu'un compartiment multiversion ne puisse être supprimé.

- Les marqueurs de suppression créés dans StorageGRID 11.7 ou version antérieure peuvent uniquement être supprimés par le biais de requêtes client S3. Ils ne sont pas supprimés par ILM, les règles de cycle de vie des compartiments ou par la suppression d'objets dans les opérations de compartiment.
- Les marqueurs de suppression d'un compartiment créé dans StorageGRID 11.8 ou une version ultérieure peuvent être supprimés par ILM, les règles de cycle de vie des compartiments, la suppression d'objets dans les opérations de compartiment ou une suppression explicite d'un client S3.

Informations associées

- "[UTILISEZ L'API REST S3](#)"
- "[Exemple 4 : règles et règles ILM pour les objets avec version S3](#)"

Créez et attribuez des niveaux de stockage dans StorageGRID

Les niveaux de stockage identifient le type de stockage utilisé par un nœud de stockage. Vous pouvez créer des classes de stockage si vous souhaitez que les règles ILM placent certains objets sur certains nœuds de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

Lorsque vous installez StorageGRID pour la première fois, le niveau de stockage **par défaut** est automatiquement attribué à chaque nœud de stockage de votre système. Si nécessaire, vous pouvez définir des niveaux de stockage personnalisés et les attribuer à différents nœuds de stockage.

L'utilisation de niveaux de stockage personnalisés vous permet de créer des pools de stockage ILM qui ne contiennent qu'un type spécifique de nœud de stockage. Vous pouvez, par exemple, stocker certains objets sur les nœuds de stockage les plus rapides, comme les appliances de stockage 100 % Flash StorageGRID.



Les nœuds de stockage contenant uniquement des métadonnées ne peuvent pas se voir attribuer un niveau de stockage. Pour plus d'informations, reportez-vous à ["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"](#). Cette sélection permet de s'assurer que le pool de stockage inclura chaque nœud de stockage sur le site, quel que soit son niveau de stockage.



Ne créez pas plus de niveaux de stockage que nécessaire. Par exemple, ne créez pas de niveau de stockage pour chaque nœud de stockage. Attribuez plutôt chaque catégorie de stockage à deux nœuds ou plus. Des types de stockage attribués à un seul nœud peuvent entraîner des backlog ILM si ce nœud est indisponible.

Étapes

1. Sélectionnez **ILM > grades de stockage**.
2. Définissez des niveaux de stockage personnalisés :
 - a. Pour chaque niveau de stockage personnalisé que vous souhaitez ajouter, sélectionnez **Insérer**  pour ajouter une ligne.
 - b. Saisissez un libellé descriptif.



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. Si vous devez modifier une étiquette enregistrée, sélectionnez **Modifier** et sélectionnez **Appliquer les modifications**.



Vous ne pouvez pas supprimer des niveaux de stockage.

3. Attribuez de nouveaux niveaux de stockage aux nœuds de stockage :

a. Repérez 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



Attribuez une note de stockage à un nœud de stockage donné une seule fois. La récupération d'un nœud de stockage suite à une défaillance permet de conserver la qualité de stockage précédemment attribuée. Ne modifiez pas cette affectation une fois la politique ILM activée. Si l'affectation est modifiée, les données sont stockées selon le nouveau niveau de stockage.

a. Sélectionnez **appliquer les modifications**.

Utiliser des pools de stockage

Découvrez les pools de stockage dans StorageGRID

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 en stockage.



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir des données et des métadonnées d'objet (nœud de stockage « combiné »), uniquement des métadonnées d'objet ou uniquement des données d'objet. Les nœuds de stockage contenant uniquement des métadonnées ne peuvent pas être utilisés dans les pools de stockage. Pour plus d'informations, reportez-vous à ["Types de nœuds de stockage"](#).

Les pools de stockage ont deux attributs :

- **Stockage** : pour les nœuds de stockage, les performances relatives du stockage de support.
- **Site** : Le centre de données où les objets sont stockés.

Les pools de stockage sont utilisés dans les règles ILM pour déterminer l'emplacement du stockage des données en mode objet et le type de stockage utilisé. Lorsque vous configurez les règles ILM pour la réplication, vous sélectionnez un ou plusieurs pools de stockage.

Directives de configuration des pools de stockage dans StorageGRID

Configurez et utilisez les pools de stockage pour vous protéger contre les pertes de données, en distribuant les données entre plusieurs sites. Les copies répliquées et les copies avec code d'effacement nécessitent différentes configurations de pool de stockage.

Consultez ["Exemples d'activation de la protection contre la perte sur site à l'aide de la réplication et du code d'effacement"](#).

Instructions pour tous les pools de stockage

- Simplifiez au maximum les configurations de vos pools de stockage. Ne créez pas plus de pools de stockage que nécessaire.
- Créez des pools de stockage avec autant de nœuds que possible. Chaque pool de stockage doit contenir deux nœuds ou plus. Un pool de stockage ne disposant pas de nœuds suffisants peut générer des arriérés ILM en cas d'indisponibilité d'un nœud.
- Évitez de créer ou d'utiliser des pools de stockage qui se chevauchent (contiennent un ou plusieurs des mêmes nœuds). Si les pools de stockage se chevauchent, il est possible d'enregistrer plusieurs copies des données d'objet sur le même nœud.
- En général, n'utilisez pas le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) ni le site tous les sites. Ces éléments sont automatiquement mis à jour pour inclure les nouveaux sites que vous ajoutez dans une extension, ce qui peut ne pas être le comportement que vous voulez.

Instructions relatives aux pools de stockage utilisés pour les copies répliquées

- Pour la protection contre la perte de site à l'aide de ["la réplication"](#), spécifiez un ou plusieurs pools de stockage spécifiques au site dans le ["Instructions de placement pour chaque règle ILM"](#).

Un pool de stockage est automatiquement créé pour chaque site lors de l'installation de StorageGRID.

L'utilisation d'un pool de stockage pour chaque site permet de placer les copies d'objets répliquées exactement là où vous en avez besoin (par exemple, une copie de chaque objet sur chaque site pour une protection contre les pertes au niveau du site).

- Si vous ajoutez un site dans une extension, créez un nouveau pool de stockage qui ne contient que le nouveau site. Ensuite, ["Mise à jour des 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 des disques entre les pools.
- Si les pools de stockage se chevauchent (contiennent les mêmes nœuds de stockage), toutes les copies de l'objet peuvent être enregistrées sur un seul site. Vous devez vous assurer que les pools de stockage sélectionnés ne contiennent pas les mêmes nœuds de stockage.

Instructions relatives aux pools de stockage utilisés pour les copies avec code d'effacement

- Pour la protection contre les pertes de site à l'aide de ["le code d'effacement"](#), créez des pools de stockage composés d'au moins trois sites. Si un pool de stockage ne comprend que deux sites, vous ne pouvez pas l'utiliser pour le code d'effacement. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage possédant deux sites.
- Le nombre de nœuds de stockage et de sites contenus dans le pool de stockage détermine ceux qui ["schémas de code d'effacement"](#) sont disponibles.

- Si possible, un pool de stockage doit inclure plus que le nombre minimum de nœuds de stockage requis pour le schéma de code d'effacement sélectionné. Par exemple, si vous utilisez un schéma de code d'effacement 6+3, vous devez avoir au moins neuf nœuds de stockage. Toutefois, il est recommandé de disposer d'au moins un nœud de stockage supplémentaire par site.
- Distribuez les nœuds de stockage sur tous les sites de façon aussi homogène que possible. Par exemple, pour prendre en charge un schéma de code d'effacement 6+3, configurez un pool de stockage qui inclut au moins trois nœuds de stockage sur trois sites.
- Si vos besoins en débit sont élevés, il n'est pas recommandé d'utiliser un pool de stockage comprenant plusieurs sites si la latence réseau entre les sites est supérieure à 100 ms. Au fur et à mesure que la latence augmente, la vitesse à laquelle StorageGRID peut créer, placer et récupérer des fragments d'objet diminue considérablement en raison de la diminution du débit du réseau TCP.

La diminution du débit affecte les taux maximaux d'ingestion et de récupération d'objets (lorsque les modes Équilibré ou Strict sont sélectionnés comme comportement d'ingestion) ou peut entraîner des engorgements de la file d'attente ILM (lorsque le mode Double validation est sélectionné comme comportement d'ingestion). Voir "[Comportement d'ingestion des règles ILM](#)".



Si votre grid ne comprend qu'un seul site, vous ne pouvez pas utiliser le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) ou le site tous les sites dans un profil de code d'effacement. Ce comportement empêche le profil de devenir non valide si un second site est ajouté.

Protection contre les pertes de site grâce aux pools de stockage dans StorageGRID

Si votre déploiement StorageGRID inclut plusieurs sites, vous pouvez utiliser la réplication et le code d'effacement avec des pools de stockage configurés de manière appropriée pour assurer la protection contre la perte de site.

Le code d'effacement et la réplication nécessitent différentes configurations de pools de stockage :

- Pour utiliser la réplication pour la protection contre les pertes sur site, utilisez les pools de stockage spécifiques au site qui sont automatiquement créés lors de l'installation de StorageGRID. Créez ensuite des règles ILM "[instructions de positionnement](#)" spécifiant plusieurs pools de stockage afin qu'une copie de chaque objet soit placée sur chaque site.
- Pour utiliser le code d'effacement pour la protection contre les pertes de site, "[créez des pools de stockage composés de plusieurs sites](#)". Ensuite, créez des règles ILM qui utilisent un pool de stockage composé de plusieurs sites et n'importe quel schéma de code d'effacement disponible.



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 "[la cohérence](#)".

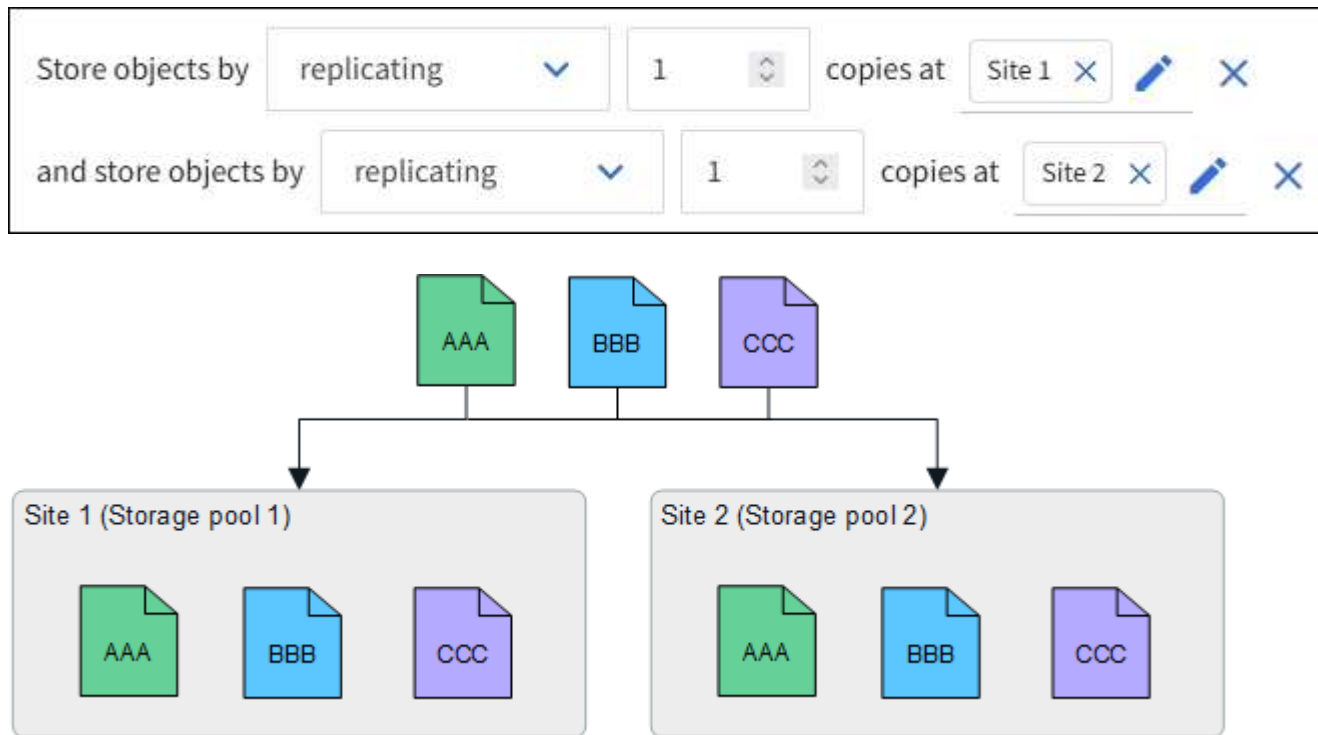
Exemple de réplication

Par défaut, un pool de stockage est créé pour chaque site lors de l'installation de StorageGRID. Avec des pools de stockage composés d'un seul site, vous pouvez configurer des règles ILM qui utilisent la réplication pour la protection contre la perte de site. Dans cet exemple :

- Le pool de stockage 1 contient le site 1
- Le pool de stockage 2 contient le site 2

- La règle ILM contient deux emplacements :
 - Stocker les objets en répliquant 1 copie sur le site 1
 - Stockez les objets en répliquant 1 copie sur le site 2

Placement des règles ILM :



Si un site est perdu, des copies des objets sont disponibles sur l'autre site.

Exemple de code d'effacement

Les pools de stockage comprenant plusieurs sites par pool de stockage vous permettent de configurer des règles ILM qui utilisent le code d'effacement pour la protection contre la perte de site. Dans cet exemple :

- Le pool de stockage 1 contient les sites 1 à 3
- La règle ILM contient un emplacement : stockage des objets par code d'effacement à l'aide d'un schéma EC 4+2 au niveau du pool de stockage 1, qui contient trois sites

Placement des règles ILM :

The screenshot shows the ILM rule configuration interface. The rule is configured to 'Store objects by erasure coding using 4+2 EC at Storage pool 1 (3 sites)'. The interface includes a dropdown menu for 'erasure coding' and a text field for the configuration.

Dans cet exemple :

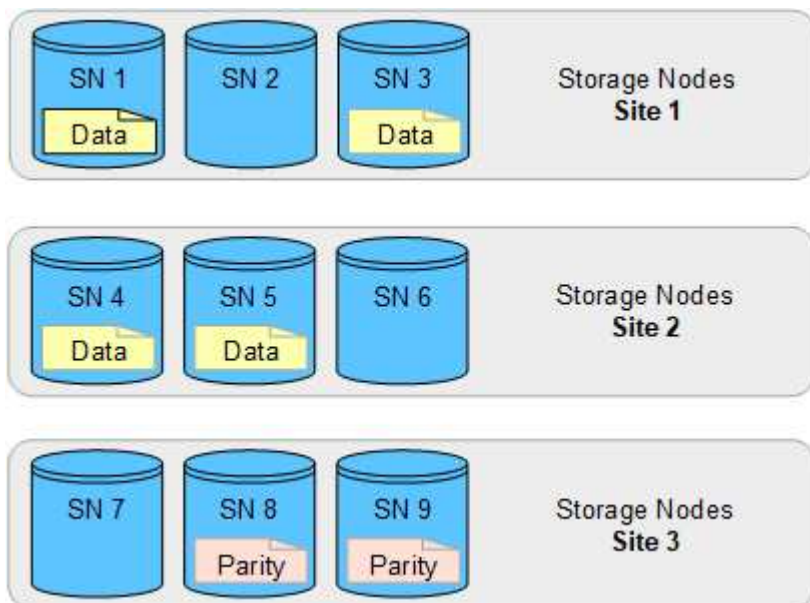
- La règle ILM utilise un schéma de code d'effacement 4+2.
- Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données d'objet.
- Chacun des six fragments est stocké sur un nœud différent sur trois sites du data Center pour assurer la

protection des données en cas de défaillance d'un nœud ou de perte d'un site.

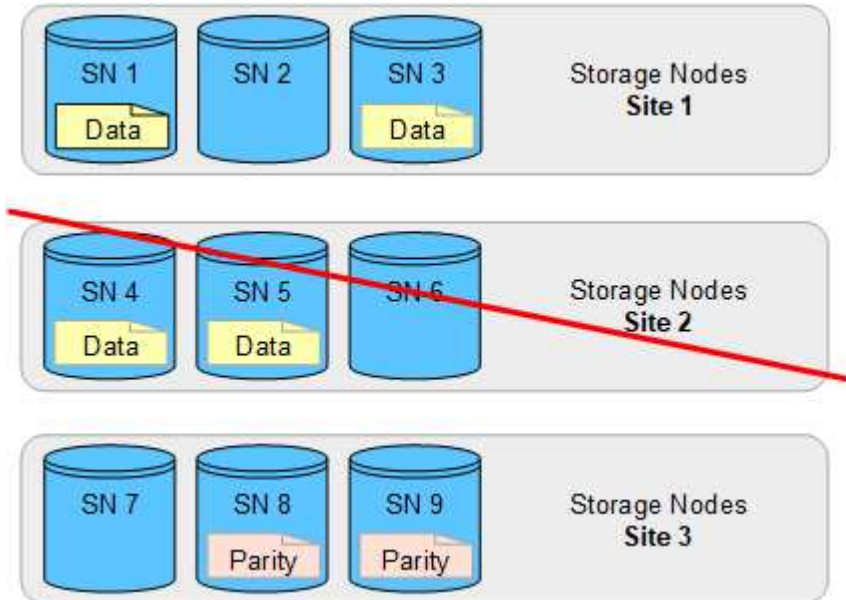


Le code d'effacement est autorisé dans les pools de stockage contenant un nombre quelconque de sites *excepté* deux sites.

Règle ILM basée sur un schéma de code d'effacement 4+2 :



En cas de perte d'un site, les données peuvent toujours être restaurées :



Créez un pool de stockage dans StorageGRID

Vous créez des pools de stockage afin de déterminer où le système StorageGRID stocke les données d'objet et le type de stockage utilisé. Chaque pool de stockage comprend un ou plusieurs sites et une ou plusieurs catégories de stockage.



Lors de l'installation de StorageGRID 12.0 ou version ultérieure sur une nouvelle grille, des pools de stockage sont automatiquement créés pour chaque site. En revanche, si vous avez initialement installé StorageGRID 11.6 ou une version antérieure, les pools de stockage ne sont pas créés automatiquement pour chaque site.

Si vous souhaitez créer des pools de stockage cloud pour stocker des données d'objet en dehors de votre système StorageGRID, reportez-vous à la section ["Informations sur l'utilisation des pools de stockage cloud"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez passé en revue les instructions relatives à la création de pools de stockage.

Description de la tâche

Les pools de stockage déterminent l'emplacement de stockage des données d'objet. Le nombre de pools de stockage dont vous avez besoin dépend du nombre de sites de votre grid et des types de copies que vous souhaitez : répliquées ou avec code d'effacement.

- Pour la réplication et le code d'effacement à un seul site, créez un pool de stockage pour chaque site. Par exemple, si vous souhaitez stocker les copies d'objets répliquées sur trois sites, créez trois pools de stockage.
- Pour le codage d'effacement sur trois sites ou plus, créez un pool de stockage comprenant une entrée pour chaque site. Par exemple, si vous souhaitez effacement d'objets de code sur trois sites, créez un pool de stockage.



N'incluez pas le site All sites dans un pool de stockage qui sera utilisé dans un profil de code d'effacement. Ajoutez plutôt une entrée distincte au pool de stockage pour chaque site qui stocke des données avec code d'effacement. Voir [cette étape](#) pour un exemple.

- Si vous avez plusieurs niveaux de stockage, ne créez pas de pool de stockage qui inclut différents niveaux de stockage sur un seul site. Voir la ["Instructions pour la création de pools de stockage"](#).

Étapes

1. Sélectionnez **ILM > pools de stockage**.

L'onglet Storage pools répertorie tous les pools de stockage définis.



Pour les nouvelles installations de StorageGRID 11.6 ou version antérieure, le pool de stockage tous les nœuds est automatiquement mis à jour chaque fois que vous ajoutez de nouveaux sites de data Center. N'utilisez pas ce pool dans les règles ILM.

2. Pour créer un nouveau pool de stockage, sélectionnez **Créer**.
3. Entrez un nom unique pour le pool de stockage. Utilisez un nom facile à identifier lorsque vous configurez les profils de code d'effacement et les règles ILM.
4. Dans la liste déroulante **site**, sélectionnez un site pour ce pool de stockage.

Lorsque vous sélectionnez un site, le nombre de nœuds de stockage du tableau est automatiquement mis à jour.

En général, n'utilisez pas le site tous les sites dans un pool de stockage. Les règles ILM utilisées par un

pool de stockage tous les sites placent les objets sur n'importe quel site disponible, ce qui vous permet de réduire le contrôle du placement des objets. En outre, un pool de stockage tous les sites utilise immédiatement les nœuds de stockage sur un nouveau site, ce qui peut ne pas être le comportement que vous attendez.

5. Dans la liste déroulante **Storage grade**, sélectionnez le type de stockage qui sera utilisé si une règle ILM utilise ce pool de stockage.

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 notes de stockage supplémentaires pour les nœuds de stockage de votre grille, elles sont répertoriées dans la liste déroulante.

6. si vous souhaitez utiliser le pool de stockage dans un profil de code d'effacement multi-site, sélectionnez **Ajouter plus de nœuds** pour ajouter une entrée pour chaque site au pool de stockage.



Vous êtes averti si vous ajoutez plusieurs entrées avec différents niveaux de stockage pour un site.

Pour supprimer une entrée, sélectionnez l'icône de suppression **X**.

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 dans StorageGRID

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 Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Étapes

1. Sélectionnez **ILM > pools de stockage**.

Le tableau Storage pools contient les informations suivantes pour chaque pool de stockage incluant des nœuds de stockage :

- **Nom** : nom d'affichage unique du pool de stockage.
- **Node count** : nombre de nœuds dans le pool de stockage.
- **Utilisation du stockage** : pourcentage de l'espace utilisable total utilisé pour les données d'objet sur ce nœud. Cette valeur n'inclut pas les métadonnées d'objet.
- **Capacité totale** : taille du pool de stockage, qui correspond à la quantité totale d'espace utilisable pour les données d'objet pour tous les nœuds du pool de stockage.
- **Utilisation ILM**: Comment le pool de stockage est actuellement utilisé. Un pool de stockage peut être inutilisé ou être utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.

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 inclut les informations suivantes pour chaque nœud :

- Nom du nœud
- Nom du site
- Qualité de stockage
- Utilisation du stockage : pourcentage de l'espace utilisable total pour les données d'objet utilisées 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 **Nœuds > Nœud de stockage > Stockage**).

4. Consultez l'onglet **ILM usage** pour déterminer si le pool de stockage est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
5. Vous pouvez également accéder à la page **ILM rules** pour en savoir plus sur les règles qui utilisent le pool de stockage et les gérer.

Voir la "[Instructions d'utilisation des règles ILM](#)".

Modifier un pool de stockage dans StorageGRID

Vous pouvez modifier un pool de stockage pour modifier son nom ou mettre à jour des sites et des notes de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez examiné le "[instructions pour la création de pools de stockage](#)".
- Si vous prévoyez de modifier un pool de stockage utilisé par une règle de la règle ILM active, vous savez comment vos modifications affectent le placement des données d'objet.

Description de la tâche

Si vous ajoutez un nouveau site ou une nouvelle classe de stockage à un pool de stockage utilisé dans la règle ILM active, sachez que les nœuds de stockage du nouveau site ou de la nouvelle classe de stockage ne seront pas utilisés automatiquement. Pour forcer StorageGRID à utiliser un nouveau site ou une nouvelle classe de stockage, vous devez activer une nouvelle règle ILM après avoir enregistré le pool de stockage modifié.

Étapes

1. Sélectionnez **ILM > pools de stockage**.
2. Cochez la case du pool de stockage à modifier.

Vous ne pouvez pas modifier le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures).

3. Sélectionnez **Modifier**.

4. Si nécessaire, modifiez le nom du pool de stockage.
5. Selon les besoins, sélectionnez d'autres sites et niveaux de stockage.

Vous ne pouvez pas modifier le site ou le niveau de stockage si le pool de stockage est utilisé dans un profil de code d'effacement et si cette modification entraînerait la non-validité du schéma de code d'effacement. Par exemple, si un pool de stockage utilisé dans un profil de code d'effacement inclut actuellement une classe de stockage avec un seul site, il est impossible d'utiliser une classe de stockage avec deux sites, car la modification rendrait le schéma de code d'effacement non valide.



L'ajout ou la suppression de sites dans un pool de stockage existant ne déplace aucune donnée codée d'effacement. Si vous souhaitez déplacer les données existantes depuis le site, vous devez créer un nouveau pool de stockage et un nouveau profil EC pour réencoder les données.

6. Sélectionnez **Enregistrer**.

Une fois que vous avez terminé

Si vous avez ajouté un nouveau site ou un 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 niveau de stockage. Par exemple, clonez votre stratégie ILM existante, puis activez le clone. Consultez ["Utilisation des règles ILM et des règles ILM"](#).

Supprimer un pool de stockage dans StorageGRID

Vous pouvez supprimer un pool de stockage qui n'est pas utilisé.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Étapes

1. Sélectionnez **ILM > pools de stockage**.
2. Consultez la colonne utilisation d'ILM du tableau pour déterminer si vous pouvez supprimer le pool de stockage.

Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé dans une règle ILM ou dans un profil de code d'effacement. Si nécessaire, sélectionnez **Storage pool name > ILM usage** pour déterminer où le pool de stockage est utilisé.

3. Si le pool de stockage que vous souhaitez supprimer n'est pas utilisé, cochez la case.
4. Sélectionnez **Supprimer**.
5. Sélectionnez **OK**.

Utilisation des pools de stockage cloud

Découvrez les Cloud Storage Pools dans StorageGRID

Un pool de stockage cloud vous permet d'utiliser ILM pour déplacer les données d'objets en dehors de votre système StorageGRID. Par exemple, vous pourriez vouloir déplacer des objets rarement consultés vers un stockage cloud à moindre coût, comme Amazon

S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le niveau d'accès Archive dans Microsoft Azure Blob Storage. Ou, vous pourriez vouloir maintenir une sauvegarde cloud des objets StorageGRID afin d'améliorer la reprise après sinistre.

Du point de vue de la gestion du cycle de vie des informations (ILM), un pool de stockage cloud est similaire à un pool de stockage. Pour stocker des objets à l'un ou l'autre emplacement, vous sélectionnez le pool lors de la création des instructions de placement d'une règle ILM. Cependant, alors que les pools de stockage sont constitués de nœuds de stockage au sein du système StorageGRID, un pool de stockage cloud est constitué d'un compartiment externe (S3) ou d'un conteneur (Azure Blob Storage).

Le tableau compare les pools de stockage aux pools de stockage cloud et montre les similarités et les différences de haut niveau.

	Pool de stockage	Pool de stockage cloud
Comment est-elle créée ?	Utilisation de l'option ILM > Storage pools dans Grid Manager.	Utilisation de l'option ILM > Storage pools > Cloud Storage pools dans Grid Manager. Vous devez configurer le compartiment ou le conteneur externe avant de pouvoir créer le pool de stockage cloud.
Combien de pools pouvez-vous créer ?	Illimitée.	Jusqu'à 10.
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage dans StorageGRID.	Dans un compartiment Amazon S3, un conteneur Azure Blob Storage ou un Google Cloud externe au système StorageGRID. Si le pool de stockage cloud est un compartiment Amazon S3 : • Vous pouvez configurer un cycle de vie de compartiment pour la transition des objets vers un stockage à long terme à faible coût, comme Amazon S3 Glacier ou S3 Glacier Deep Archive. Le système de stockage externe doit prendre en charge la classe de stockage Glacier et l'API RestoreObject S3. • 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 Azure Blob Storage, StorageGRID transfère l'objet vers le niveau Archive. Remarque : En général, ne configurez pas la gestion du cycle de vie d'Azure Blob Storage pour le conteneur utilisé pour un pool de stockage cloud. RestoreObject opérations sur les objets dans le pool de stockage cloud peuvent être affectées par le cycle de vie configuré.

	Pool de stockage	Pool de stockage cloud
Quels sont les contrôles du placement des objets ?	Règle ILM dans les politiques ILM actives.	Règle ILM dans les politiques ILM actives.
Quelle est la méthode de protection des données utilisée ?	La réplication ou le code d'effacement.	La réplication.
Combien de copies de chaque objet sont autorisées ?	Plusieurs.	Une copie dans le pool de stockage cloud et, éventuellement, une ou plusieurs copies dans StorageGRID. Remarque : vous ne pouvez pas stocker un objet dans plusieurs pools de stockage cloud à un moment donné.
Quels sont les avantages ?	Les objets sont rapidement accessibles à tout moment.	Stockage à moindre coût Remarque : les données FabricPool ne peuvent pas être hiérarchisées vers des pools de stockage cloud.

Cycle de vie d'un objet Cloud Storage Pool dans StorageGRID

Avant d'implémenter les pools de stockage cloud, vérifiez le cycle de vie des objets stockés dans chaque type de pool de stockage cloud.

S3 : cycle de vie d'un objet de pool de stockage cloud

Les étapes décrivent les étapes de cycle de vie d'un objet stocké dans un pool de stockage cloud S3.



« Glacier » fait référence à la classe de stockage Glacier et 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 bloc ou standard est prise en charge.



Google Cloud Platform (GCP) prend en charge la récupération d'objets à partir d'un stockage à long terme sans nécessiter de POST-restauration.

1. Objet stocké dans StorageGRID

Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. Objet déplacé vers le pool de stockage cloud S3

- Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud S3 en tant qu'emplacement, StorageGRID déplace l'objet vers le compartiment S3 externe spécifié par le pool de stockage cloud.

- Une fois l'objet déplacé vers le pool de stockage cloud S3, l'application client peut le récupérer à l'aide d'une requête GetObject S3 de StorageGRID, sauf si l'objet a été transféré vers le stockage Glacier.

3. L'objet a été transféré vers Glacier (état non récupérable)

- L'objet peut également être transféré vers le stockage Glacier. Par exemple, un compartiment S3 externe peut utiliser la configuration du cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après quelques jours.



Si vous souhaitez effectuer la transition d'objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et qui prend en charge l'API S3 RestoreObject.

- Pendant la transition, l'application client peut utiliser une requête S3 HeadObject pour contrôler l'état de l'objet.

4. Objet restauré à partir du stockage Glacier

Si un objet a été transféré vers le stockage Glacier, l'application client peut émettre une demande RestoreObject S3 pour restaurer une copie récupérable dans le pool de stockage cloud S3. La demande spécifie le nombre de jours pendant lesquels la copie doit être disponible dans le pool de stockage cloud et le Tier d'accès aux données à utiliser pour l'opération de restauration (accéléré, Standard ou en bloc). Lorsque la date d'expiration de la copie récupérable est atteinte, la copie est automatiquement renvoyée à un état non récupérable.



Si une ou plusieurs copies de l'objet existent également sur les nœuds de stockage dans StorageGRID, il n'est pas nécessaire de restaurer l'objet à partir de Glacier en émettant une requête RestoreObject. À la place, 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 client 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 de cycle de vie d'un objet stocké dans un pool de stockage cloud Azure.

1. Objet stocké dans StorageGRID

Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. Objet déplacé vers Azure Cloud Storage Pool

Lorsque l'objet correspond à une règle ILM qui utilise un pool de stockage cloud Azure comme emplacement de placement, StorageGRID déplace l'objet vers le conteneur Azure Blob Storage externe spécifié par le Cloud Storage Pool.

3. L'objet a été transféré au niveau Archive (état non récupérable)

Immédiatement après le déplacement de l'objet vers le pool de stockage cloud Azure, StorageGRID transfère automatiquement l'objet vers le niveau d'archivage du stockage Blob Azure.

4. Objet restauré à partir du niveau d'archive

Si un objet a été transféré vers le niveau Archive, l'application client peut émettre une requête S3 RestoreObject pour restaurer une copie récupérable vers Azure Cloud Storage Pool.

Lorsque StorageGRID reçoit la requête RestoreObject, il transfère temporairement l'objet vers le niveau Cool d'Azure Blob Storage. Dès que la date d'expiration indiquée dans la requête RestoreObject est atteinte, StorageGRID transfère l'objet vers le 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 aux archives en émettant une requête RestoreObject. À la place, 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 Azure Cloud Storage Pool, l'application client peut émettre une requête GetObject pour récupérer l'objet restauré.

Informations associées

["UTILISEZ L'API REST S3"](#)

Cas d'utilisation des Cloud Storage Pool dans StorageGRID

À l'aide des pools de stockage cloud, vous pouvez sauvegarder ou hiérarchiser les données vers un emplacement externe. En outre, vous pouvez sauvegarder ou déplacer des données vers plusieurs clouds.

Sauvegardez les données StorageGRID dans un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder des objets StorageGRID dans un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, vous pouvez utiliser les données objet du pool de stockage cloud pour transmettre les requêtes des clients. Cependant, vous devrez peut-être émettre une requête S3 RestoreObject pour accéder à la copie d'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objet d'un pool de stockage cloud peuvent également être utilisées pour restaurer des données perdues à partir de StorageGRID en raison d'un volume de stockage ou d'une défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

Pour implémenter une solution de sauvegarde :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour stocker simultanément les copies d'objets sur les nœuds de stockage (en tant que copies répliquées ou avec code d'effacement) et une seule copie objet dans le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Déplacez les données de StorageGRID vers un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour stocker des objets en dehors du système StorageGRID. Supposons par exemple que vous disposez d'un grand nombre d'objets que vous devez conserver, mais que vous prévoyez d'accéder rarement à ces objets. Un pool de stockage cloud permet de classer les objets en fonction de leur coût de stockage et de libérer de l'espace dans StorageGRID.

Pour implémenter une solution de hiérarchisation :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour déplacer les objets rarement utilisés depuis les nœuds de stockage vers le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Possibilité de gérer plusieurs terminaux cloud

Vous pouvez configurer plusieurs points de terminaison de Cloud Storage Pool si vous souhaitez hiérarchiser ou sauvegarder des données d'objets sur plusieurs clouds. Les filtres de vos règles ILM vous permettent de spécifier quels objets sont stockés dans chaque Cloud Storage Pool. Par exemple, vous pouvez stocker des objets de certains locataires ou compartiments dans Amazon S3 Glacier et des objets d'autres locataires ou compartiments dans Azure Blob Storage. Ou, vous pouvez déplacer des données entre Amazon S3 Glacier et Azure Blob Storage.



Lors de l'utilisation de plusieurs terminaux Cloud Storage Pool, n'oubliez pas qu'un objet ne peut être stocké que dans un seul pool de stockage cloud à la fois.

Pour implémenter plusieurs terminaux cloud :

1. Créez jusqu'à 10 pools de stockage cloud.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment opportun dans chaque pool de stockage cloud. Par exemple, stockage des objets du compartiment A dans le pool de stockage cloud A, stockage des objets du compartiment B dans le pool de stockage cloud B. stockage cloud ou stockage des objets dans le pool de stockage cloud A pendant un certain temps, puis déplacement des objets vers le pool de stockage cloud B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simuler et activer la règle.

Exigences et limites des Cloud Storage Pool dans StorageGRID

Si vous envisagez d'utiliser un pool de stockage cloud pour déplacer les objets hors du système StorageGRID, vous devez étudier les critères de configuration et d'utilisation des pools de stockage cloud.

Considérations générales

- En général, le stockage d'archives cloud, tel que Amazon S3 Glacier ou Azure Blob Storage, est un endroit peu coûteux pour stocker des données d'objets. Cependant, les coûts de récupération des données depuis le stockage d'archives cloud sont relativement élevés. Pour obtenir le coût global le plus bas, vous devez prendre en compte quand et à quelle fréquence vous accéderez aux objets dans le Cloud Storage Pool. L'utilisation d'un Cloud Storage Pool 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 ajoutée pour extraire un objet de la cible du pool de stockage cloud.

- Les objets avec le verrouillage d'objet S3 activé ne peuvent pas être placés dans les pools de stockage cloud.
- Les combinaisons de plateforme, d'authentification et de protocoles suivantes avec le verrouillage objet S3 ne sont pas prises en charge pour les pools de stockage cloud :
 - **Plateformes** : Google Cloud Platform et Azure
 - **Types d'authentification** : Accès anonyme
 - **Protocole** : HTTP

Considérations relatives aux ports utilisés pour les pools de stockage cloud

Pour s'assurer que les règles ILM peuvent déplacer des objets vers et depuis le pool de stockage cloud spécifié, vous devez configurer le ou les réseaux contenant les nœuds de stockage du système. Vous devez vous assurer que les ports suivants peuvent communiquer avec le pool de stockage cloud.

Par défaut, les pools de stockage cloud utilisent les ports suivants :

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

Vous pouvez spécifier un autre port lorsque vous créez ou modifiez un pool de stockage cloud.

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

Considérations relatives aux coûts

L'accès au stockage dans le cloud à l'aide d'un pool de stockage cloud requiert une connectivité réseau au cloud. Tenez compte des coûts de l'infrastructure réseau que vous utiliserez pour accéder au cloud et le provisionner de façon appropriée, en fonction de la quantité de données que vous prévoyez de déplacer entre StorageGRID et le cloud à l'aide du pool de stockage cloud.

Lorsque StorageGRID se connecte au terminal Cloud Storage Pool externe, plusieurs demandes de contrôle de la connectivité sont émises et les opérations nécessaires sont possibles. Un certain nombre de coûts supplémentaires seront associés à ces demandes, mais le coût de la surveillance d'un pool de stockage cloud ne doit être qu'une fraction du coût global du stockage d'objets dans S3 ou Azure.

Des coûts plus importants peuvent être encourus si vous devez déplacer des objets depuis un terminal externe de pool de stockage dans le cloud vers StorageGRID. Les objets peuvent être redéplacés vers StorageGRID dans l'un ou l'autre de ces cas :

- La seule copie de l'objet se trouve dans un pool de stockage cloud et vous décidez de le stocker dans StorageGRID à la place. Dans ce cas, vous reconfigurez vos règles et votre règle ILM. Lors de l'évaluation ILM, StorageGRID émet plusieurs demandes de récupération de l'objet à partir du pool de stockage cloud. StorageGRID crée ensuite le nombre spécifié de copies répliquées ou codées en local. Une fois que l'objet est de nouveau déplacé vers StorageGRID, la copie dans le pool de stockage cloud est supprimée.
- Les objets sont perdus en raison de la défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.



Lorsque les objets sont déplacés vers StorageGRID à partir d'un pool de stockage cloud, StorageGRID émet plusieurs requêtes vers le terminal de pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, contactez le support technique pour obtenir de l'aide pour estimer le délai et les coûts associés.

S3 : autorisations requises pour le compartiment de pool de stockage cloud

Les règles du compartiment S3 externe utilisé pour un pool de stockage cloud doivent accorder l'autorisation StorageGRID pour déplacer un objet vers le compartiment, obtenir l'état d'un objet, restaurer un objet depuis le stockage Glacier, le cas échéant, etc. Dans l'idéal, StorageGRID doit disposer d'un accès contrôle total au compartiment (`s3:*`). Toutefois, si ce n'est pas possible, la politique de compartiment doit accorder les autorisations S3 suivantes à StorageGRID :

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3 : considérations sur le cycle de vie du compartiment externe

Le déplacement d'objets entre StorageGRID et le compartiment S3 externe spécifié dans le pool de stockage cloud est contrôlé par des règles ILM et les règles ILM actives dans StorageGRID. À l'inverse, la transition des objets à partir du compartiment S3 externe spécifié dans le pool de stockage cloud vers Amazon S3 Glacier ou S3 Glacier Deep Archive (ou vers une solution de stockage implémentant la classe de stockage Glacier) est contrôlée par la configuration du cycle de vie de ce compartiment.

Si vous souhaitez effectuer la transition d'objets à partir de Cloud Storage Pool, vous devez créer la configuration de cycle de vie appropriée sur le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API `S3 RestoreObject`.

Supposons par exemple que vous souhaitiez que tous les objets déplacés d'StorageGRID vers le pool de stockage cloud soient transférés immédiatement vers le stockage Amazon S3 Glacier. Vous devez créer une configuration de cycle de vie sur le compartiment S3 externe qui spécifie une seule action (**transition**) comme suit :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Cette règle consiste à basculer tous les objets de compartiment vers Amazon S3 Glacier le jour de leur création (à savoir le jour où ils ont été déplacés d'StorageGRID vers le pool de stockage cloud).



Lors de la configuration du cycle de vie du compartiment externe, n'utilisez jamais les actions **expiration** pour définir quand les objets arrivent à expiration. Les actions d'expiration entraînent la suppression des objets expirés par le système de stockage externe. Si vous tentez par la suite d'accéder à un objet expiré à partir de StorageGRID, l'objet supprimé est introuvable.

Si vous souhaitez transférer des objets du pool de stockage cloud vers le service S3 Glacier Deep Archive (au lieu d'Amazon S3 Glacier), spécifiez le `<StorageClass>DEEP_ARCHIVE</StorageClass>` cycle de vie du compartiment. Cependant, notez que vous ne pouvez pas utiliser le Expedited Tier pour restaurer des objets à partir 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. Lorsque vous créez un compte de stockage à utiliser avec un pool de stockage cloud, vous devez utiliser le Tier actif comme niveau par défaut. Même si StorageGRID définit immédiatement le Tier sur Archive lors du déplacement d'objets vers le pool de stockage cloud, l'utilisation du paramètre par défaut de Hot garantit que vous ne serez pas facturé de frais de suppression anticipé pour les objets supprimés du Tier Cool avant le minimum de 30 jours.

Azure : gestion du cycle de vie non prise en charge

N'utilisez pas la gestion du cycle de vie d'Azure Blob Storage pour le conteneur utilisé avec un Cloud Storage Pool. Les opérations de cycle de vie pourraient interférer avec les opérations du Cloud Storage Pool.

Informations associées

["Création d'un pool de stockage cloud"](#)

Pools de stockage cloud et réplication CloudMirror dans StorageGRID

Lorsque vous commencez à utiliser les pools de stockage cloud, il peut être utile d'étudier les similarités et les différences entre les pools de stockage cloud et le service de réplication StorageGRID CloudMirror.

	Pool de stockage cloud	Service de réplication CloudMirror
Quel est l'objectif principal ?	Sert de cible d'archivage. La copie d'objet du pool de stockage cloud peut être la seule copie de l'objet ou une copie supplémentaire. Ainsi, au lieu de conserver deux copies sur site, vous pouvez conserver une copie dans StorageGRID et en envoyer une autre dans le pool de stockage cloud.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). Crée une copie indépendante d'un objet dans une infrastructure S3 indépendante.
Comment est-il configuré ?	Défini de la même manière que les pools de stockage, à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Peut être sélectionné comme emplacement dans une règle ILM. Lorsqu'un pool de stockage est constitué d'un groupe de nœuds de stockage, un pool de stockage cloud est défini à l'aide d'un terminal S3 ou Azure distant (adresse IP, identifiants, etc.).	Utilisateur locataire " Configure la réplication CloudMirror " en définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. Une fois le terminal CloudMirror configuré, tous les compartiments appartenant à ce compte peuvent être configurés pour pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	En général, un administrateur grid	Généralement, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Tier Azure Blob Archive • Google Cloud Platform (GCP)	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
Pourquoi déplacer des objets vers la destination ?	Une ou plusieurs règles ILM dans les politiques ILM actives. Les règles ILM définissent le déplacement des objets StorageGRID vers le pool de stockage cloud et le déplacement des objets.	Acte d'ingestion d'un nouvel objet dans un compartiment source configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été modifiés.

	Pool de stockage cloud	Service de réplication CloudMirror
Comment les objets sont-ils récupérés ?	Les applications doivent demander à StorageGRID de récupérer les objets qui ont été déplacés vers un pool de stockage cloud. Si la seule copie d'un objet a été transférée vers le stockage d'archivage, StorageGRID gère le processus de restauration de l'objet afin de pouvoir la récupérer.	Étant donné que la copie en miroir dans le compartiment de destination est une copie indépendante, les applications peuvent récupérer l'objet en effectuant des demandes vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.
Pouvez-vous lire directement depuis la destination ?	Non. Les objets déplacés vers un pool de stockage cloud sont gérés par StorageGRID. Les demandes de lecture doivent être dirigées vers StorageGRID (et StorageGRID sera responsable de la récupération à partir du pool de stockage cloud).	Oui, car la copie en miroir est une copie indépendante.
Que se passe-t-il si un objet est supprimé de la source ?	L'objet est également supprimé du pool de stockage cloud.	L'action de suppression n'est pas répliquée. Un objet supprimé n'existe plus dans le compartiment StorageGRID, mais il continue d'exister dans le compartiment de destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.
Comment accéder aux objets après un incident (le système StorageGRID n'est pas opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Au cours de ce processus, les copies des objets répliqués peuvent être restaurées à l'aide de copies dans le pool de stockage cloud.	Les copies d'objets de la destination CloudMirror sont indépendantes de StorageGRID, ce qui permet d'y accéder directement avant la restauration des nœuds StorageGRID.

Créez un Cloud Storage Pool dans StorageGRID

Un pool de stockage cloud spécifie un seul compartiment Amazon S3 externe, un autre fournisseur compatible S3 ou un conteneur Azure Blob Storage.

Lorsque vous créez un Cloud Storage Pool, 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 (Amazon S3/GCP ou Azure Blob Storage), ainsi que les informations dont StorageGRID a besoin pour accéder au compartiment ou au conteneur externe.

StorageGRID valide le pool de stockage cloud dès que vous le sauvegardez. Vous devez donc vous assurer

que le compartiment ou le conteneur spécifié dans le pool de stockage cloud est accessible et qu'il existe.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille 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 compartiment ou conteneur externe référencé par le pool de stockage cloud existe déjà, et vous disposez du [informations sur le terminal de service](#).
- Pour accéder au godet ou au conteneur, vous avez le [informations de compte pour le type d'authentification](#) choix.

Étapes

1. Sélectionnez **ILM > Storage pools > Cloud Storage pools**.
2. Sélectionnez **Créer**, puis entrez les informations suivantes :

Champ	Description
Nom du pool de stockage cloud	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Nom facile à identifier lors de la configuration des règles ILM.
Type de fournisseur	Quel fournisseur de cloud utiliser pour ce pool de stockage cloud : • Amazon S3/GCP : sélectionnez cette option pour Amazon S3, commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou un autre fournisseur compatible avec S3. • Stockage Azure Blob
Seau ou conteneur	Nom du compartiment S3 ou du conteneur Azure externe. Vous ne pouvez pas modifier cette valeur une fois le pool de stockage cloud enregistré.

3. en fonction de votre sélection de type de fournisseur, entrez les informations sur le noeud final du service.

Amazon S3/GCP

- a. Pour le protocole, sélectionnez HTTPS ou HTTP.



N'utilisez pas de connexions HTTP pour les données sensibles.

- b. Entrez le nom d'hôte. Exemple :

`s3-aws-region.amazonaws.com`

- c. Sélectionnez le style d'URL :

Option	Description
Détection automatique	Essayez de détecter automatiquement le style d'URL à utiliser, en fonction des informations fournies. Par exemple, si vous spécifiez une adresse IP, StorageGRID utilise une URL de style de chemin d'accès. Sélectionnez cette option uniquement si vous ne savez pas quel style spécifique utiliser.
De type hébergement virtuel	Utilisez une URL de type hébergement virtuel pour accéder au compartiment. Les URL de type hébergement virtuel incluent le nom de compartiment dans le nom de domaine. Exemple : <code>https://bucket-name.s3.company.com/key-name</code>
Style de trajectoire	Utilisez une URL de style de chemin d'accès pour accéder au compartiment. Les URL de type chemin d'accès incluent le nom du compartiment à la fin Exemple : <code>https://s3.company.com/bucket-name/key-name</code> Note: l'option URL de style chemin d'accès n'est pas recommandée et sera obsolète dans une future version de StorageGRID.

- d. Vous pouvez également saisir le numéro de port ou utiliser le port par défaut : 443 pour HTTPS ou 80 pour HTTP.

Stockage Azure Blob Storage

- a. À l'aide de l'un des formats suivants, entrez l'URI du point de terminaison de service.

- `https://host:port`
- `http://host:port`

Exemple : `https://myaccount.blob.core.windows.net:443`

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour HTTPS et le port 80 pour HTTP.

4. sélectionnez **continue**. Sélectionnez ensuite le type d'authentification et entrez les informations requises pour le terminal Cloud Storage Pool :

Touche d'accès

Pour Amazon S3/GCP ou tout autre fournisseur compatible avec S3

- a. **ID de la clé d'accès** : saisissez l'ID de la clé d'accès du compte propriétaire du compartiment externe.
- b. **Clé d'accès secrète** : saisissez la clé d'accès secrète.

Rôles IAM n'importe où

Pour le service AWS IAM Roles Anywhere

StorageGRID utilise AWS Security Token Service (STS) pour générer de manière dynamique un jeton de courte durée afin d'accéder aux ressources AWS.

- a. **Région AWS IAM Roles Anywhere** : sélectionnez la région du pool de stockage cloud. Par exemple `us-east-1`, .
- b. **Trust ancre URN** : saisissez l'URN de l'ancre de confiance qui valide les demandes d'informations d'identification STS à courte durée de vie. Peut être une AC racine ou intermédiaire.
- c. **Profil URN** : saisissez l'URN du profil IAM Roles Anywhere qui répertorie les rôles qui sont présumés pour toute personne de confiance.
- d. **Rôle URN** : saisissez l'URN du rôle IAM qui est assurable pour 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 au plus 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. S'il est 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** : clé privée du certificat de l'entité finale.

CAP (portail d'accès C2S)

Pour le service S3 de 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 du serveur CAP, y compris tous les paramètres d'API requis et facultatifs attribués à votre compte C2S.
- b. **Certificat de l'autorité de certification du serveur** : sélectionnez **Parcourir** et téléchargez le certificat de l'autorité de certification que StorageGRID utilisera pour vérifier le serveur CAP. Le certificat doit être codé au format PEM et émis par une autorité de certification gouvernementale (AC) appropriée.
- c. **Certificat client** : sélectionnez **Parcourir** et téléchargez le certificat que StorageGRID utilisera pour s'identifier sur le serveur CAP. Le certificat client doit être codé au format PEM, délivré par une autorité de certification gouvernementale (CA) appropriée et accordé l'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 cryptée, entrez la phrase de passe pour déchiffrer la clé privée du

client. Sinon, laissez le champ **phrase de passe de clé privée client** vide.



Si le certificat client est crypté, utilisez le format traditionnel pour le chiffrement. Le format chiffré PKCS #8 n'est pas pris en charge.

Stockage Azure Blob Storage

Pour Azure Blob Storage, clé partagée uniquement

- a. **Nom du compte** : saisissez le nom du compte de stockage qui possède le conteneur externe
- b. **Clé de compte** : saisissez la clé secrète du compte de stockage

Utilisez 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
Utilisez les certificats d'autorité de certification racine dans le système d'exploitation du nœud de stockage	Utilisez les certificats CA de la grille installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. Sélectionnez Parcourir et téléchargez le certificat codé PEM.
Ne vérifiez pas le certificat	Si vous sélectionnez cette option, 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 :

- Vérifie que le compartiment ou le conteneur et le terminal de service existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
- Écrit un fichier de marqueur dans le compartiment ou le conteneur pour l'identifier en tant que pool de stockage cloud. Ne supprimez jamais ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment ou le conteneur que vous avez spécifié n'existe pas déjà.

7. Si une erreur se produit, consultez le "[Instructions de dépannage des pools de stockage cloud](#)", résolvez les problèmes, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Informations associées

["Ports utilisés pour les communications externes"](#)

Afficher les détails du pool de stockage cloud dans StorageGRID

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 Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **ILM > Storage pools > Cloud Storage pools**.

Le tableau pools de stockage cloud inclut les informations suivantes pour chaque pool de stockage cloud, y compris les nœuds de stockage :

- **Nom** : le nom d'affichage unique du pool.
- **URI** : l'identificateur de ressource uniforme du pool de stockage cloud.
- **Type de fournisseur** : quel fournisseur de cloud est utilisé pour ce pool de stockage cloud.
- **Container** : nom du compartiment utilisé pour le pool de stockage cloud.
- **Utilisation ILM**: Comment le pool est actuellement utilisé. Un pool de stockage cloud peut être inutilisé ou être utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.
- **Dernière erreur** : dernière erreur détectée lors d'une vérification de l'intégrité 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 du pool s'affiche.

3. Consultez l'onglet **Authentication** pour en savoir plus sur le type d'authentification pour ce pool de stockage cloud et pour modifier les détails de l'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 certificat PEM.
5. Consultez l'onglet **ILM usage** pour déterminer si le pool de stockage cloud est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
6. Vous pouvez également accéder à la page **ILM rules** ["découvrez et gérez toutes les règles"](#) qui utilise le pool de stockage cloud.

Modifier un Cloud Storage Pool dans StorageGRID

Vous pouvez modifier un pool de stockage cloud pour modifier son nom, le point de terminaison de service ou d'autres informations. Cependant, vous ne pouvez pas modifier le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez examiné le ["Considérations relatives aux pools de stockage cloud"](#).

Étapes

1. Sélectionnez **ILM > Storage pools > Cloud Storage pools**.

Le tableau Cloud Storage pools répertorie les pools de stockage cloud existants.

2. Cochez la case correspondant au pool de stockage cloud à modifier, 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 terminal du service, les paramètres d'authentification ou la méthode de vérification du certificat.



Vous ne pouvez pas modifier le type de fournisseur, le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Si vous avez déjà téléchargé un certificat de serveur ou de client, vous pouvez développer l'accordéon **Certificate Details** pour examiner le certificat actuellement utilisé.

4. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID valide la présence du compartiment ou du conteneur et du terminal de service, et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche. Par exemple, une erreur peut être signalée en cas d'erreur de certificat.

Reportez-vous aux instructions de "[Résolution des problèmes avec les pools de stockage cloud](#)", résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Supprimer un Cloud Storage Pool dans StorageGRID

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 Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[autorisations d'accès requises](#)".

Si nécessaire, utilisez la règles ILM pour déplacer les données d'objet

Si le pool de stockage cloud que vous souhaitez supprimer contient des données d'objet, vous devez utiliser ILM pour déplacer les données vers un autre emplacement. Par exemple, vous pouvez déplacer les données vers des nœuds de stockage sur votre grille ou vers un autre pool de stockage cloud.

Étapes

1. Sélectionnez **ILM > Storage pools > Cloud Storage pools**.

2. Consultez la colonne utilisation ILM du tableau pour déterminer si vous pouvez supprimer le pool de stockage cloud.

Vous ne pouvez pas supprimer un pool de stockage cloud s'il est utilisé dans une règle ILM ou dans un profil de code d'effacement.

3. Si le pool de stockage cloud est utilisé, sélectionnez **cloud Storage pool name > ILM usage**.
4. ["Clonez chaque règle ILM"](#) Qui place actuellement les objets dans le pool de stockage cloud que vous souhaitez supprimer.
5. Déterminez l'emplacement où vous souhaitez déplacer les objets existants gérés par chaque règle clonée.

Vous pouvez utiliser un ou plusieurs pools de stockage ou un autre pool de stockage cloud.

6. Editez chacune des règles que vous avez clonées.

Pour l'étape 2 de l'assistant Créer une règle ILM, sélectionnez le nouvel emplacement dans le champ **copies AT**.

7. ["Création d'une règle ILM"](#) et remplacez chacune des anciennes règles par une règle clonée.
8. Activer la nouvelle règle.
9. Attendez que ILM supprime les objets du pool de stockage cloud et les place à un nouvel emplacement.

Supprimer le pool de stockage cloud

Lorsque le pool de stockage cloud est vide et qu'il n'est utilisé dans aucune règle ILM, vous pouvez le supprimer.

Avant de commencer

- Vous avez supprimé toutes les règles ILM qui auraient pu utiliser le pool.
- Vous avez confirmé que le compartiment S3 ou le conteneur Azure ne contient aucun objet.

Une erreur se produit si vous tentez de supprimer un pool de stockage cloud s'il contient des objets. Voir ["Résoudre les problèmes liés aux pools de stockage cloud"](#).



Lorsque vous créez un pool de stockage cloud, StorageGRID écrit un fichier de marqueur vers le compartiment ou le conteneur pour l'identifier comme un pool de stockage cloud. Ne supprimez pas ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

Étapes

1. Sélectionnez **ILM > Storage pools > Cloud Storage pools**.
2. Si la colonne utilisation d'ILM indique que Cloud Storage Pool n'est pas utilisé, cochez la case.
3. Sélectionnez **actions > Supprimer**.
4. Sélectionnez **OK**.

Dépanner les pools de stockage cloud dans StorageGRID

Suivez ces étapes de dépannage pour résoudre les erreurs que vous pouvez rencontrer lors de la création, de la modification ou de la suppression d'un pool de stockage cloud.

Déterminez si une erreur s'est produite

StorageGRID effectue un simple contrôle de l'état de santé de chaque pool de stockage cloud en lisant l'objet connu `x-ntap-sgws-cloud-pool-uuid` pour s'assurer que le pool de stockage cloud est accessible et qu'il fonctionne correctement. Lorsque StorageGRID rencontre une erreur sur le noeud final, il vérifie l'état de santé toutes les minutes depuis chaque noeud de stockage. Une fois l'erreur résolue, les vérifications de l'état de

santé s'arrêtent. Si une vérification de l'état de santé détecte un problème, un message s'affiche dans la colonne dernière erreur du tableau pools de stockage cloud de la page pools de stockage cloud.

Le tableau indique la dernière erreur détectée pour chaque pool de stockage cloud et indique la durée de l'erreur.

En outre, une alerte **erreur** de connectivité de pool de stockage cloud est déclenchée si le contrôle d'intégrité détecte qu'une ou plusieurs nouvelles erreurs de pool de stockage cloud se sont produites au cours des 5 dernières minutes. Si vous recevez une notification par e-mail pour cette alerte, accédez à la page Storage pools (sélectionnez **ILM > Storage pools**), consultez les messages d'erreur dans la colonne Last error (dernière erreur) et reportez-vous aux instructions de dépannage ci-dessous.

Vérifiez si une erreur a été résolue

Après avoir résolu les problèmes sous-jacents, vous pouvez déterminer si l'erreur a été résolue. Sur la page Cloud Storage Pool, sélectionnez le nœud final, puis sélectionnez **Clear error**. Un message de confirmation indique que StorageGRID a résolu l'erreur pour le pool de stockage cloud.

Si le problème sous-jacent a été résolu, le message d'erreur ne s'affiche plus. Toutefois, si le problème sous-jacent n'a pas été résolu (ou si une erreur différente est rencontrée), le message d'erreur s'affiche dans la colonne dernière erreur dans les minutes qui suivent.

Erreur : échec de la vérification de l'état de santé. Erreur du nœud final

Vous pourriez rencontrer cette erreur dans l'un des cas suivants :

- Lorsque vous activez le verrouillage d'objets S3 avec la rétention par défaut pour votre compartiment Amazon S3 après avoir commencé à utiliser ce compartiment comme pool de stockage cloud. Cette erreur se produit lorsque l'opération PUT ne comporte pas d'en-tête HTTP avec une valeur de somme de contrôle de la charge utile, telle que `Content-MD5`. Cette valeur d'en-tête est requise par AWS pour les opérations PUT dans des compartiments avec le verrouillage d'objets S3 activé.

Pour corriger ce problème, suivez les étapes dans "[Modifiez un pool de stockage cloud](#)" sans apporter de modifications. Cette action déclenche la validation de la configuration du Cloud Storage Pool qui détecte et met à jour automatiquement l'indicateur S3 Object Lock sur la configuration du point de terminaison du Cloud Storage Pool.

- Lorsque vous activez le verrouillage d'objet S3 avec la rétention par défaut pour votre compartiment StorageGRID S3 après avoir commencé à utiliser ce compartiment pour un pool de stockage cloud.

Pour corriger ce problème :

- Si vous utilisez HTTP : les pools de stockage cloud avec S3 Object Lock activé ne sont pas pris en charge. Modifiez la connexion du point de terminaison pour utiliser HTTPS à la place.
- Si vous utilisez HTTPS : suivez les étapes dans "[Modifiez un pool de stockage cloud](#)" sans apporter de modifications. Cette action déclenche la validation de la configuration du Cloud Storage Pool qui détecte et met à jour automatiquement l'indicateur S3 Object Lock sur la configuration du point de terminaison du Cloud Storage Pool.

En cas de problème supplémentaire, contactez le support technique.

Erreur : ce pool de stockage cloud contient du contenu inattendu

Cette erreur peut se produire lorsque vous tentez de créer, modifier ou supprimer un pool de stockage cloud. Cette erreur se produit si le compartiment ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` fichier

de marqueur, mais que ce fichier ne possède pas le champ de métadonnées avec l'UUID attendu.

En général, cette erreur s'affiche uniquement si vous créez un pool de stockage cloud et qu'une autre instance de StorageGRID utilise déjà le même pool de stockage cloud.

Essayez l'une des étapes suivantes pour corriger le problème :

- Si vous configurez un nouveau pool de stockage cloud et que le compartiment contient le `x-ntap-sgws-cloud-pool-uuid` fichier et les clés d'objet supplémentaires, comme dans l'exemple suivant, créez un nouveau compartiment et utilisez ce nouveau compartiment.

Exemple de clé d'objet supplémentaire : `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si le `x-ntap-sgws-cloud-pool-uuid` fichier est le seul objet du compartiment, supprimez ce fichier.

Si ces étapes ne s'appliquent pas à votre scénario, contactez l'assistance.

Erreur : impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du noeud final

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 plateforme, une authentification ou une combinaison de protocoles non pris 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, consultez le message d'erreur du noeud final.

- Si le message d'erreur contient `Get url: EOF`, vérifiez que le terminal de service utilisé pour le pool de stockage cloud n'utilise pas HTTP pour un conteneur ou un compartiment qui nécessite HTTPS.
- Si le message d'erreur contient `Get url: net/http: request canceled while waiting for connection`, vérifiez que la configuration réseau 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 plateforme, une authentification ou un protocole non pris en charge, passez à une configuration prise en charge avec le verrouillage objet S3 et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
- Pour tous les autres messages d'erreur de point final, essayez un ou plusieurs des éléments suivants :
 - Créez un conteneur ou un compartiment externe avec le même nom que vous avez saisi pour le Cloud Storage Pool, et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
 - Corrigez le nom de conteneur ou de compartiment que vous avez spécifié pour le pool de stockage cloud, et essayez de sauvegarder à nouveau le nouveau pool de stockage cloud.

Erreur : échec de l'analyse du certificat CA

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. L'erreur se produit si StorageGRID n'a pas pu analyser le certificat que vous avez saisi lors de la configuration du pool de stockage cloud.

Pour corriger le problème, vérifiez si le certificat CA que vous avez fourni ne présente pas de problèmes.

Erreur : un pool de stockage cloud associé à cet ID est introuvable

Cette erreur peut se produire lorsque vous essayez de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le noeud final renvoie une réponse 404, ce qui peut signifier l'un des éléments suivants :

- Les identifiants utilisés pour le pool de stockage cloud ne disposent pas des autorisations de lecture pour le compartiment.
- Le compartiment utilisé pour le pool de stockage cloud n'inclut pas le `x-ntap-sgws-cloud-pool-uuid` fichier de marqueur.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée possède les autorisations requises.
- Modifiez le pool de stockage cloud avec des identifiants disposant des autorisations requises.
- Si les autorisations sont correctes, contactez l'assistance technique.

Erreur : impossible de vérifier le contenu du pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID de lire le contenu du compartiment Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur du noeud final.

Erreur : les objets ont déjà été placés dans ce compartiment

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Vous ne pouvez pas supprimer un pool de stockage cloud s'il contient des données qui y ont été déplacées par ILM, des données qui se trouvaient dans le compartiment avant la configuration du pool de stockage cloud, ou des données qui ont été placées dans le compartiment par une autre source après la création du pool de stockage cloud.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Suivez les instructions pour déplacer de nouveau des objets vers StorageGRID dans la section « cycle de vie d'un objet de pool de stockage cloud ».
- Si vous êtes certain que les objets restants n'ont pas été placés dans le pool de stockage cloud par ILM, supprimez manuellement les objets du compartiment.



Ne supprimez jamais manuellement d'objets d'un pool de stockage cloud qui auraient pu y avoir été placés par ILM. Si vous tentez par la suite d'accéder à un objet supprimé manuellement à partir de StorageGRID, l'objet supprimé est introuvable.

Erreur : le proxy a rencontré une erreur externe lors de la tentative d'accès au pool de stockage cloud

Cette erreur peut se produire si vous avez configuré un proxy de stockage non transparent entre les nœuds de stockage et le terminal S3 externe utilisé pour le pool de stockage cloud. Cette erreur se produit si le serveur proxy externe ne parvient pas à atteindre le terminal Cloud Storage Pool. Par exemple, il se peut que le serveur DNS ne puisse pas résoudre le nom d'hôte ou qu'il existe un problème de réseau externe.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez les paramètres de Cloud Storage Pool (**ILM > Storage pools**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Erreur : le certificat X.509 est hors période de validité

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur se produit lorsque l'authentification nécessite un certificat X.509 pour s'assurer 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 vers le pool de stockage cloud.
- Assurez-vous que toute alerte d'expiration de certificat relative à ce pool de stockage cloud est résolue.

Informations associées

["Cycle de vie d'un objet de pool de stockage cloud"](#)

Gérez les profils de code d'effacement dans StorageGRID

Vous pouvez afficher les détails d'un profil de code d'effacement et renommer un profil si nécessaire. Vous pouvez désactiver un profil de code d'effacement s'il n'est actuellement utilisé dans aucune règle ILM.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Afficher les détails du profil de code d'effacement

Vous pouvez afficher les détails d'un profil de code d'effacement pour déterminer son état, le schéma de code 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 s'affiche.
3. Vous pouvez également afficher l'onglet règles ILM pour obtenir la liste des règles ILM qui utilisent le profil, ainsi que les règles ILM qui les utilisent.
4. Vous pouvez également afficher l'onglet nœuds de stockage pour plus de détails sur chaque nœud de stockage du pool de stockage du profil, par exemple le site où il se trouve et l'utilisation du stockage.

Renommer un profil de code d'effacement

Vous pouvez renommer un profil de code d'effacement pour le rendre plus évident.

Étapes

1. Sélectionnez **Configuration > Système > Codage d'effacement**.

2. Sélectionnez le profil à renommer.
3. Sélectionnez **Renommer**.
4. Entrez un nom unique pour le profil de code d'effacement.

Le nom du profil de code d'effacement est ajouté au nom du pool de stockage dans l'instruction de placement d'une règle ILM.



Les noms des profils de code d'effacement doivent être uniques. Une erreur de validation se produit si vous utilisez le nom d'un profil existant, même si ce profil a été désactivé.

5. Sélectionnez **Enregistrer**.

Désactiver un profil de code d'effacement

Vous pouvez désactiver un profil de code d'effacement si vous ne prévoyez plus de l'utiliser et si ce profil n'est pas utilisé dans les règles ILM.



Vérifier qu'aucune réparation de données avec code d'effacement ou procédure de désaffectation n'est en cours. Un message d'erreur s'affiche si vous tentez de désactiver un profil de code d'effacement alors que l'une de ces opérations est en cours.

Description de la tâche

StorageGRID vous empêche de désactiver un profil de code d'effacement si l'une des conditions suivantes est vraie :

- Le profil de code d'effacement est actuellement utilisé dans une règle ILM.
- Le profil de code d'effacement n'est plus utilisé dans les règles ILM, mais les données en objet et les fragments de parité du profil existent toujours.

Étapes

1. Sélectionnez **Configuration > Système > Codage d'effacement**.
2. Dans l'onglet actif, consultez la colonne **Status** pour confirmer que le profil de code d'effacement que vous souhaitez désactiver n'est utilisé dans aucune règle ILM.

Vous ne pouvez pas désactiver un profil de code d'effacement s'il est utilisé dans une règle ILM. Dans cet exemple, le profil Data Center 1 2+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, effectuez la procédure suivante :
 - a. Sélectionnez **ILM > règles**.
 - b. Sélectionnez chaque règle et consultez le diagramme de rétention pour déterminer si la règle utilise le profil de code d'effacement que vous souhaitez désactiver.

- c. Si la règle ILM utilise le profil de code d'effacement que vous souhaitez désactiver, déterminez si cette règle est utilisée dans une règle ILM.
- d. Complétez les étapes supplémentaires du tableau, en fonction de l'endroit où le profil de code d'effacement est utilisé.

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
Jamais utilisé dans une règle ILM	Aucune étape supplémentaire n'est requise. Poursuivre cette procédure.	<i>Aucun</i>
Les règles ILM n'ont jamais été utilisées dans toutes les règles ILM	i. Modifiez ou supprimez toutes les règles ILM affectées. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. ii. Poursuivre cette procédure.	"Utilisation des règles ILM et des règles ILM"
Règle ILM actuellement dans une règle ILM active	i. Cloner la règle. ii. Suppression de la règle ILM utilisant le profil de code d'effacement iii. Ajoutez une ou plusieurs nouvelles règles ILM pour assurer la protection des objets. iv. Enregistrez, simulez et activez la nouvelle stratégie. v. Attendez que la nouvelle stratégie soit appliquée et que les objets existants soient déplacés vers de nouveaux emplacements en fonction des nouvelles règles que vous avez ajoutées. Remarque : en fonction du nombre d'objets et de la taille de votre système StorageGRID, le déplacement des objets vers de nouveaux emplacements peut prendre des semaines, voire des mois, en fonction des nouvelles règles ILM. Bien que vous puissiez tenter en toute sécurité de désactiver un profil de code d'effacement alors qu'il est toujours associé à des données, l'opération de désactivation échoue. Un message d'erreur vous informe si le profil n'est pas encore prêt à être désactivé. vi. Modifiez ou supprimez la règle que vous avez supprimée de la stratégie. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. vii. Poursuivre cette procédure.	"Créer une règle ILM" "Utilisation des règles ILM et des règles ILM"

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
Dans une règle ILM actuellement dans une politique ILM	i. Modifiez la stratégie. ii. Suppression de la règle ILM utilisant le profil de code d'effacement iii. Ajoutez une ou plusieurs nouvelles règles ILM pour protéger tous les objets. iv. Enregistrez la stratégie. v. Modifiez ou supprimez la règle que vous avez supprimée de la stratégie. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. vi. Poursuivre cette procédure.	"Créer une règle ILM" "Utilisation des règles ILM et des règles ILM"

e. Actualisez la page Erasure-Coding Profiles 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 code d'effacement s'affiche.



Vous pouvez sélectionner plusieurs profils à désactiver en même temps, tant que chaque profil n'est utilisé dans aucune règle.

5. Si vous êtes sûr de vouloir désactiver le profil, sélectionnez **Désactiver**.

Résultats

- Si StorageGRID peut désactiver le profil de code d'effacement, son état est désactivé. Vous ne pouvez plus sélectionner ce profil pour une règle ILM. Vous ne pouvez pas réactiver un profil désactivé.
- Si StorageGRID ne peut pas désactiver le profil, un message d'erreur s'affiche. Par exemple, un message d'erreur s'affiche si les données d'objet sont toujours associées à ce profil. Vous devrez peut-être attendre plusieurs semaines avant d'essayer à nouveau le processus de désactivation.

Configurer les régions S3 pour StorageGRID

Les règles ILM peuvent filtrer les objets en fonction des régions facultatives 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 à utiliser par les compartiments du système.



Vous ne pouvez pas modifier la région d'un compartiment après sa création.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

Lorsque vous créez un compartiment S3, vous pouvez spécifier une région. La spécification d'une région permet au compartiment d'être géographiquement proche de ses utilisateurs, ce qui peut contribuer à optimiser la latence, réduire les coûts et satisfaire aux exigences réglementaires.

Lorsque vous créez une règle ILM, vous pouvez utiliser la région associée à un compartiment S3 comme filtre avancé. Par exemple, vous pouvez concevoir une règle qui s'applique uniquement aux objets dans des compartiments S3 créés dans la `us-west-2` région. Afin d'optimiser la latence, vous pouvez ensuite placer des copies de ces objets sur des nœuds de stockage sur un site de data Center dans cette région.

Lors de la configuration de régions, suivez les consignes suivantes :

- Par défaut, tous les compartiments sont considérés comme appartenant à la `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.
- Lors de la création du compartiment S3, vous devez utiliser le nom exact de la région. Les noms de région sont sensibles à la casse. Les caractères autorisés sont des chiffres, des lettres et des tirets.



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 affectée à une stratégie (active ou inactive).
- Si vous utilisez une région non valide en tant que filtre avancé dans une règle ILM, vous ne pouvez pas ajouter cette règle à une règle.

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 devez ajouter de nouveau la région si vous souhaitez utiliser le filtre avancé contrainte d'emplacement pour trouver des objets dans ce compartiment.

Étapes

1. Sélectionnez **ILM > régions**.

La page Régions apparaît.

2. Sélectionnez l'onglet **Toutes les régions** ou **Région par défaut**.

Toutes les régions

L'onglet **Toutes les régions** répertorie les régions actuellement définies, y compris la région par défaut définie.



Vous ne pouvez pas supprimer ou modifier la région par défaut dans l'onglet **Toutes les régions**. Utilisez l'onglet **Région par défaut** pour modifier la région par défaut.

- a. Pour ajouter une région, sélectionnez **Ajouter une autre région**.
- b. Entrez le nom d'une région à utiliser lors de la création de compartiments S3.

Vous devez utiliser ce nom de région exact comme élément de demande LocationConstraint lorsque vous créez le compartiment S3 correspondant.

- c. Pour supprimer une zone inutilisée, sélectionnez l'icône de suppression .

Un message d'erreur s'affiche si vous tentez de supprimer une région actuellement utilisée dans une stratégie (active ou inactive).

- d. Une fois les modifications effectuées, sélectionnez **Enregistrer**.

Vous pouvez maintenant sélectionner ces régions dans la section filtres avancés de l'étape 1 de l'assistant de création de règles ILM. Voir "[Utilisation de filtres avancés dans les règles ILM](#)".

Région par défaut

L'onglet **Région par défaut** affiche la région par défaut actuellement définie, que vous pouvez modifier.

- a. Pour modifier la région par défaut, sélectionnez le nom de la région parmi les options disponibles dans la liste déroulante **Région par défaut**.
- b. Sélectionnez **Enregistrer**.

Création d'une règle ILM

Découvrez les règles ILM dans StorageGRID

Pour gérer les objets, vous créez un ensemble de règles de gestion du cycle de vie des informations (ILM) et vous les organisez en une règle ILM.

Chaque objet ingéré dans le système est évalué par rapport à la règle active. Lorsqu'une règle de la règle correspond aux métadonnées d'un objet, les instructions de la règle déterminent les actions que StorageGRID prend pour copier et stocker cet objet.



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

Éléments d'une règle ILM

Une règle ILM comporte trois éléments :

- **Critères de filtrage** : les filtres de base et avancés d'une règle définissent les objets auxquels la règle s'applique. Si un objet correspond à tous les filtres, StorageGRID applique la règle et crée les copies d'objet spécifiées dans les instructions de placement de la règle.
- **Instructions de placement** : les instructions de placement d'une règle définissent le nombre, le type et l'emplacement des copies d'objet. Chaque règle peut inclure une séquence d'instructions de placement pour modifier le nombre, le type et l'emplacement des copies d'objet au fil du temps. À l'expiration de la période de temps pour un placement, les instructions du placement suivant sont automatiquement appliquées par l'évaluation ILM suivante.
- **Comportement d'ingestion** : le comportement d'ingestion d'une règle vous permet de choisir la façon dont les objets filtrés par la règle sont protégés lors de leur ingestion (lorsqu'un client S3 enregistre un objet dans la grille).

Filtrage de règles ILM

Lorsque vous créez une règle ILM, vous spécifiez des filtres pour identifier les objets auxquels la règle s'applique.

Dans le cas le plus simple, une règle ne peut pas utiliser de filtres. Toute règle qui n'utilise pas de filtre s'applique à tous les objets. Elle doit donc être la dernière règle (par défaut) d'une politique ILM. La règle par défaut fournit des instructions de stockage pour les objets qui ne correspondent pas aux filtres d'une autre règle.

- Les filtres de base vous permettent d'appliquer différentes règles à de grands groupes d'objets distincts. Ces filtres vous permettent d'appliquer une règle à des comptes de locataire spécifiques, à des compartiments S3 spécifiques, ou aux deux.

Les filtres de base vous permettent d'appliquer facilement différentes règles à un grand nombre d'objets. Par exemple, les données financières de votre entreprise peuvent être stockées pour répondre à la réglementation, tandis que les données du service marketing doivent être stockées pour faciliter les opérations quotidiennes. Après avoir créé des comptes de tenant distincts pour chaque service ou après avoir séparé les données des différents services dans des compartiments S3 distincts, vous pouvez facilement créer une règle qui s'applique à tous les enregistrements financiers et une deuxième règle qui s'applique à toutes les données de marketing.

- Les filtres avancés vous offrent un contrôle granulaire. Vous pouvez créer des filtres pour sélectionner des objets en fonction des propriétés d'objet suivantes :
 - Temps d'ingestion
 - Heure du dernier accès
 - Tout ou partie du nom de l'objet (clé)
 - Contrainte d'emplacement (S3 uniquement)
 - Taille de l'objet
 - Métadonnées d'utilisateur
 - Balise objet (S3 uniquement)

Vous pouvez filtrer les objets selon des critères très spécifiques. Par exemple, les objets stockés par le service d'imagerie de l'hôpital peuvent être utilisés fréquemment s'ils ont moins de 30 jours et rarement par la suite, tandis que les objets contenant les informations relatives aux visites des patients peuvent devoir être copiés

dans le service de facturation du siège social du réseau de santé. Vous pouvez créer des filtres qui identifient chaque type d'objet en fonction du nom, de la taille, des balises d'objet S3 ou de tout autre critère pertinent. Il crée ensuite des règles distinctes pour stocker chaque ensemble d'objets de façon appropriée.

Vous pouvez combiner des filtres selon vos besoins dans une seule règle. Par exemple, le service marketing pourrait souhaiter stocker des fichiers d'images volumineux différemment des dossiers de fournisseurs, tandis que le service des ressources humaines pourrait avoir besoin de stocker les dossiers du personnel dans une zone géographique spécifique et des informations sur les politiques de manière centralisée. Dans ce cas, vous pouvez créer des règles qui filtrent par compte de locataire pour séparer les enregistrements de chaque service, tout en utilisant des filtres dans chaque règle pour identifier le type spécifique d'objets auquel la règle s'applique.

Instructions de placement des règles ILM

Les instructions de placement déterminent l'emplacement, le moment et le mode de stockage des données objet. Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps.

Lorsque vous créez des instructions de positionnement :

- Vous commencez par spécifier l'heure de référence, qui détermine le début des instructions de positionnement. L'heure de référence peut être lorsqu'un objet est ingéré, lorsqu'un objet est accédé, lorsqu'un objet versionné devient non courant ou une heure définie par l'utilisateur.
- Vous spécifiez ensuite le moment où le placement s'appliquera, par rapport à l'heure de référence. Par exemple, un placement peut commencer le jour 0 et se poursuivre pendant 365 jours, par rapport à l'ingestion de l'objet.
- Enfin, vous spécifiez le type de copies (réplication ou codage d'effacement) et l'emplacement de stockage des copies. Par exemple, vous pouvez stocker deux copies répliquées sur deux sites différents.

Chaque règle peut définir plusieurs placements pour une période unique et différents placements pour différentes périodes.

- Pour placer des objets à plusieurs emplacements pendant une seule période, sélectionnez **Ajouter un autre type ou un autre emplacement** pour ajouter plus d'une ligne pour cette période.
- Pour placer des objets à différents emplacements dans différentes périodes, sélectionnez **Ajouter une autre période** pour ajouter la période suivante. Spécifiez ensuite une ou plusieurs lignes dans la période.

L'exemple illustre deux instructions de positionnement sur la page Define stages de l'assistant Create ILM Rule.

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

1

Add other type or location

Time period 2
From Day store forever

Store objects by copies at

2

Add other type or location

La première consigne de placement 1 comporte deux lignes pour la première année :

- La première ligne crée deux copies d'objets répliquées sur deux sites de data Center.
- La deuxième ligne crée une copie avec code d'effacement 6+3 sur tous les sites de data Center.

La deuxième instruction de placement 2 crée deux copies après un an et les conserve indéfiniment.

Lorsque vous définissez l'ensemble des instructions de placement pour une règle, vous devez vous assurer qu'au moins une instruction de placement commence au jour 0, qu'il n'y a pas d'écart entre les périodes que vous avez définies, et que l'instruction de placement final continue soit indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

À chaque expiration de la règle, les instructions de placement de contenu pour la période suivante sont appliquées. De nouvelles copies d'objet sont créées et les copies inutiles sont supprimées.

Comportement d'ingestion des règles ILM

Le comportement d'ingestion détermine si les copies d'objet sont immédiatement placées conformément aux instructions de la règle, ou si des copies intermédiaires sont effectuées et que les instructions de placement sont appliquées ultérieurement. Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Équilibré** : StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.
- **Dual commit** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Informations associées

- ["Options d'ingestion"](#)
- ["Avantages, inconvénients et limites des options d'acquisition"](#)
- ["Impact de la cohérence et des règles ILM pour la protection des données"](#)

Exemple de règle ILM

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

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

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

Informations associées

- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Qu'est-ce qu'un pool de stockage cloud"](#)

Accédez à l'assistant de création de règle ILM dans StorageGRID

Les règles ILM permettent de gérer le placement des données d'objet au fil du temps. Pour créer une règle ILM, l'assistant de création d'une règle ILM est utilisé.



Si vous souhaitez créer la règle ILM par défaut d'une règle, suivez la procédure ["Instructions de création d'une règle ILM par défaut"](#) à la place.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Si vous souhaitez spécifier les comptes de tenant auxquels cette règle s'applique, vous avez ["Droits d'accès aux comptes de locataires"](#) ou vous connaissez l'ID de compte de chaque compte.
- Si vous souhaitez que la règle filtre les objets sur les métadonnées de l'heure du dernier accès, les mises à jour de l'heure du dernier accès doivent être activées par le compartiment S3.
- Vous avez configuré tous les pools de stockage cloud que vous prévoyez d'utiliser. Voir ["Création d'un pool de stockage cloud"](#).
- Vous connaissez le ["options d'ingestion"](#).
- Si vous devez créer une règle conforme pour l'utiliser avec le verrouillage objet S3, vous connaissez bien le ["Conditions requises pour le verrouillage d'objet S3"](#).

- En option, vous avez regardé la vidéo :

[Aperçu des règles de l'ILM](#)

Description de la tâche

Lors de la création de règles ILM :

- Comparez la topologie et les configurations de stockage du système StorageGRID.
- Tenez compte des types de copies d'objet à effectuer (répliquées ou avec code d'effacement) et du nombre de copies de chaque objet requises.
- Déterminez les types de métadonnées d'objet utilisés dans les applications qui se connectent au système StorageGRID. Les règles ILM filtrent les objets en fonction de leurs métadonnées.
- Réfléchissez à l'emplacement souhaité pour le stockage des copies d'objets au fil du temps.
- Choisissez l'option d'ingestion à utiliser (équilibrée, stricte ou Dual commit).

Étapes

1. Sélectionnez **ILM > règles**.
2. Sélectionnez **Créer**. "[Étape 1 \(entrer les détails\)](#)" De l'assistant de création d'une règle ILM s'affiche.

Saisissez les détails et les filtres d'une règle ILM StorageGRID

L'étape **entrer détails** de l'assistant Créer une règle ILM vous permet d'entrer un nom et une description pour la règle et de définir des filtres pour la règle.

La saisie d'une description et la définition de filtres pour la règle sont facultatives.

Description de la tâche

Lors de l'évaluation d'un objet "[Règle ILM](#)" par rapport à un , StorageGRID compare les métadonnées de l'objet aux filtres de la règle. Si les métadonnées correspondent à tous les filtres, StorageGRID utilise la règle pour placer l'objet. Vous pouvez concevoir une règle à appliquer à tous les objets, ou spécifier des filtres de base, tels qu'un ou plusieurs comptes de locataire, noms de compartiment ou filtres avancés, tels que la taille de l'objet ou les métadonnées utilisateur.

Étapes

1. Entrez un nom unique pour la règle dans le champ **Nom**.
2. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.

Vous devez décrire le but ou la fonction de la règle afin de pouvoir reconnaître la règle ultérieurement.

3. Vous pouvez également sélectionner un ou plusieurs comptes de 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 compte de locataire, vous ne pouvez pas sélectionner de locataires dans la liste. Entrez plutôt l'ID de tenant ou entrez plusieurs ID comme une chaîne délimitée par des virgules.

4. Vous pouvez également spécifier les compartiments S3 auxquels cette règle s'applique.

Si **s'applique à tous les compartiments** est sélectionné (par défaut), la règle s'applique à tous les compartiments S3.

5. Pour les locataires S3, sélectionnez **Oui** pour appliquer la règle uniquement aux anciennes versions d'objets dans des compartiments S3 pour lesquels la gestion de versions est activée.

Si vous sélectionnez **Oui**, "Noncurrent Time" sera automatiquement sélectionné pour l'heure de référence dans "Étape 2 de l'assistant de création de règles ILM".



Une heure non actuelle s'applique uniquement aux objets S3 dans des compartiments avec gestion des versions. Voir "Opérations sur les godets, PutBucketVersioning" et "Gestion des objets avec le verrouillage d'objets S3".

Vous pouvez utiliser cette option pour réduire l'impact du stockage des objets multiversion en filtrant pour les versions d'objets non à jour. Voir "Exemple 4 : règles et règles ILM pour les objets avec version S3".

6. Si vous le souhaitez, sélectionnez **Ajouter un filtre avancé** pour spécifier des filtres supplémentaires.

Si vous ne configurez pas le filtrage avancé, la règle s'applique à tous les objets correspondant aux filtres de base. Pour plus d'informations sur le filtrage avancé, reportez-vous aux sections [Utilisation de filtres avancés dans les règles ILM](#) et [Spécifiez plusieurs types et valeurs de métadonnées](#).

7. Sélectionnez **Continuer**. "Étape 2 (définir les placements)" De l'assistant de création d'une règle ILM s'affiche.

Utilisation de filtres avancés dans les règles ILM

Le filtrage avancé vous permet de créer des règles ILM qui s'appliquent uniquement à des objets spécifiques en fonction de leurs métadonnées. Lorsque vous configurez le filtrage avancé d'une règle, vous sélectionnez le type de métadonnées que vous souhaitez associer, sélectionnez un opérateur et spécifiez une valeur de métadonnées. Lors de l'évaluation des objets, la règle ILM s'applique uniquement aux objets dont les métadonnées correspondent au filtre avancé.

Le tableau indique les types de métadonnées que vous pouvez spécifier dans les filtres avancés, les opérateurs que vous pouvez utiliser pour chaque type de métadonnées et les valeurs de métadonnées attendues.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Temps d'ingestion	- est - n'est pas - est avant - est activé ou avant - est après - est activé ou après	Heure et date d'ingestion de l'objet. Remarque : pour éviter les problèmes de ressources lors de l'activation d'une nouvelle stratégie ILM, vous pouvez utiliser le filtre avancé heure d'ingestion dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion sur une valeur supérieure ou égale à la durée approximative de l'entrée en vigueur de la nouvelle règle pour vous assurer que les objets existants ne sont pas déplacés inutilement.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Clé	• égal à • n'est pas égal • contient • ne contient pas • commence par • ne commence pas par • se termine par • ne se termine pas par	Tout ou partie d'une clé d'objet S3 unique. Par exemple, vous pouvez souhaiter faire correspondre des objets qui se terminent <code>.txt</code> par ou commencent par <code>test-object/</code>.
Heure du dernier accès	• est • n'est pas • est avant • est activé ou avant • est après • est activé ou après	Heure et date de la dernière récupération de l'objet (lecture ou visualisation). Remarque : si vous prévoyez d'"utiliser l'heure du dernier accès"utiliser un filtre avancé, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3.
Contrainte d'emplacement (S3 uniquement)	• égal à • n'est pas égal	Région dans laquelle un compartiment S3 a été créé. Utilisez ILM > régions pour définir les régions affichées. 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 S3".
Taille de l'objet	• égal à • n'est pas égal • inférieur à • inférieur ou égal à • supérieur à • supérieur ou égal à	Taille de l'objet. Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Métadonnées d'utilisateur	• contient • se termine par • égal à • existe • commence par • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par	Paire clé-valeur, où Nom métadonnées utilisateur est la clé et valeur métadonnées la valeur. Par exemple, pour filtrer les objets qui ont des métadonnées utilisateur de <code>color=blue</code>, spécifiez <code>color</code> Nom de métadonnées utilisateur, <code>equals</code> pour l'opérateur et <code>blue</code> valeur de métadonnées. Remarque : les noms de métadonnées de l'utilisateur ne sont pas sensibles à la casse; les valeurs de métadonnées de l'utilisateur sont sensibles à la casse.
Balise objet (S3 uniquement)	• contient • se termine par • égal à • existe • commence par • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par	Paire clé-valeur, où Nom balise objet est la clé et valeur balise objet est la valeur. Par exemple, pour filtrer sur des objets dont la balise d'objet est <code>Image=True</code>, spécifiez <code>Image</code> Nom de la balise d'objet, <code>equals</code> pour l'opérateur et <code>True</code> pour valeur de la balise d'objet. Remarque : les noms de balise d'objet et les valeurs de balise d'objet sont sensibles à la casse. Vous devez entrer ces éléments exactement comme ils ont été définis pour l'objet.

Spécifiez plusieurs types et valeurs de métadonnées

Lorsque vous définissez le filtrage avancé, vous pouvez spécifier plusieurs types de métadonnées et plusieurs valeurs de métadonnées. Par exemple, si vous souhaitez qu'une règle corresponde à des objets d'une taille comprise entre 10 Mo et 100 Mo, vous devez sélectionner le type de métadonnées **Object size** et spécifier deux valeurs de métadonnées.

- La première valeur de métadonnées spécifie des objets supérieurs ou égaux à 10 Mo.
- La seconde valeur de métadonnées spécifie des objets inférieurs ou égaux à 100 Mo.

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size
▼

greater than or equal to
▼

10
▼

MB
▼

X

and

Object size
▼

less than or equal to
▼

100
▼

MB
▼

X

L'utilisation de plusieurs entrées vous permet d'avoir un contrôle précis sur les objets à associer. Dans

l'exemple suivant, la règle s'applique aux objets dont la marque A ou la marque B est la valeur des métadonnées de l'utilisateur camera_type. Toutefois, la règle s'applique uniquement aux objets de marque B dont la taille est inférieure à 10 Mo.

The screenshot shows the configuration for an ILM rule with two filter groups:

- Filter group 1:** Objects with all of following metadata will be evaluated by this rule:
 - User metadata (dropdown) equals (dropdown) Brand A (text box)
- or**
- Filter group 2:** Objects with all of following metadata will be evaluated by this rule:
 - User metadata (dropdown) equals (dropdown) Brand B (text box)
 - and** Object size (dropdown) less than or equal to (dropdown) 10 (text box) MB (dropdown)

Each filter group has a link to "Add another advanced filter".

Définir les instructions de placement pour une règle StorageGRID ILM

L'étape **Define stages** de l'assistant Create ILM Rule vous permet de définir les instructions de placement qui déterminent la durée de stockage des objets, le type de copies (répliquées ou avec code d'effacement), l'emplacement de stockage et le nombre de copies.



Les captures d'écran illustrées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID.

Description de la tâche

Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps. Lorsque vous utilisez plusieurs instructions, les périodes doivent être contiguës et au moins une instruction doit commencer le jour 0. Les instructions peuvent se poursuivre indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

Chaque instruction de placement peut avoir plusieurs lignes si vous voulez créer différents types de copies ou utiliser différents emplacements au cours de cette période.

Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une copie répliquée sur le site 2 pour la première année. Après un an, une copie avec code d'effacement pour 2+1 est effectuée et enregistrée sur un seul site.

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 **temps de référence**, sélectionnez le type de temps à utiliser lors du calcul de l'heure de début d'une instruction de placement.

Option	Description
Temps d'ingestion	Heure à laquelle l'objet a été ingéré.
Heure du dernier accès	Heure à laquelle l'objet a été récupéré pour la dernière fois (lu ou affiché). Pour utiliser cette option, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3. Reportez-vous à la "Utiliser l'heure du dernier accès dans les règles ILM".
Heure de création définie par l'utilisateur	Heure spécifiée dans les métadonnées définies par l'utilisateur.
Heure non actuelle	"Heure non actuelle" est automatiquement sélectionné si vous avez sélectionné Oui pour la question, "appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée)?" dans "Étape 1 de l'assistant de création de règles ILM" .

Si vous souhaitez créer une règle *complice*, vous devez sélectionner **heure d'ingestion**. Reportez-vous à la ["Gestion des objets avec le verrouillage d'objets S3"](#).

2. Dans la section **période et placements**, entrez une heure de début et une durée pour la première période.

Par exemple, vous pouvez spécifier l'emplacement de stockage des objets pour la première année (*du magasin du jour 0 pendant 365 jours*). Au moins une instruction doit commencer au jour 0.

3. Pour créer des copies répliquées :

- a. Dans la liste déroulante **stocker les objets par**, sélectionnez **répliquer**.
- b. Sélectionnez le nombre de copies à effectuer.

Un avertissement s'affiche si vous changez le nombre de copies en 1. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Reportez-vous à la ["Pourquoi ne pas utiliser la réplication à copie unique"](#).

Pour éviter ce risque, effectuez une ou plusieurs des actions suivantes :

- Augmentez le nombre de copies pour la période.
- Ajoutez des copies à d'autres pools de stockage ou à un pool de stockage cloud.
- Sélectionnez **code d'effacement** au lieu de **répliquer**.

Vous pouvez ignorer cet avertissement en toute sécurité si cette règle crée déjà plusieurs copies pour toutes les périodes.

- c. Dans le champ **copies AT**, sélectionnez les pools de stockage à ajouter.

Si vous spécifiez un seul pool de stockage, sachez que StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si votre grille comprend trois nœuds de stockage et que vous sélectionnez 4 comme nombre de copies, seules trois copies seront faites—une copie pour chaque nœud de stockage.

L'alerte **ILM placement inaccessible** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Si vous spécifiez plus d'un pool de stockage, gardez ces règles à l'esprit :

- Le nombre de copies ne peut pas être supérieur au nombre de pools de stockage.
- Si le nombre de copies équivaut au nombre de pools de stockage, une copie de l'objet est stockée dans chaque pool de stockage.
- Si le nombre de copies est inférieur au nombre de pools de stockage, une copie est stockée sur le site d'ingestion, puis le système distribue les copies restantes afin de maintenir un équilibre entre l'utilisation du disque dans les pools, tout en veillant à ce qu'aucun site ne reçoive plus d'une copie d'un objet.
- Si les pools de stockage se chevauchent (contiennent les mêmes nœuds de stockage), toutes les copies de l'objet peuvent être enregistrées sur un seul site. Par conséquent, ne spécifiez pas le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) et un autre pool de stockage.

4. Pour créer une copie avec code d'effacement :

- a. Dans la liste déroulante **stocker les objets par**, sélectionnez **code d'effacement**.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

- b. Si vous n'avez pas ajouté de filtre de taille d'objet pour une valeur supérieure à 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 à ajouter et le schéma de code d'effacement à utiliser.

L'emplacement de stockage d'une copie avec code d'effacement comprend le nom du schéma de code d'effacement, suivi du nom du pool de stockage.

Les schémas de code d'effacement disponibles sont limités par le nombre de nœuds de stockage dans le pool de stockage que vous sélectionnez. Un **Recommended** badge apparaît à côté des schémas qui fournissent le ["protection optimale ou réduction des surcharges de stockage"](#).

5. Facultatif :

- a. Sélectionnez **Ajouter un autre type ou un autre emplacement** pour créer des copies supplémentaires à différents emplacements.
- b. Sélectionnez **Ajouter une autre période** pour ajouter différentes périodes.



Les suppressions d'objets se produisent en fonction des paramètres suivants :

- Les objets sont automatiquement supprimés à la fin de la période finale, sauf si une autre période se termine par **Forever**.
- Selon ["paramètres de période de conservation des compartiments et des locataires"](#) la , les objets peuvent ne pas être supprimés, même si la période de conservation ILM se termine.

6. Pour stocker des objets dans un pool de stockage cloud :

- a. Dans la liste déroulante **stocker les objets par**, sélectionnez **répliquer**.
- b. Sélectionnez le champ **copies at**, puis sélectionnez un pool de stockage cloud.

Lorsque vous utilisez des pools de stockage cloud, gardez ces règles à l'esprit :

- Vous ne pouvez pas sélectionner plusieurs pools de stockage cloud dans une instruction de placement unique. De même, vous ne pouvez pas sélectionner un pool de stockage cloud et un pool de stockage dans la même instruction de placement.
- Vous ne pouvez stocker qu'une seule copie d'un objet dans un pool de stockage cloud donné. Un message d'erreur s'affiche si vous définissez **copies** sur 2 ou plus.
- Vous ne pouvez pas stocker plusieurs copies d'objet simultanément dans un pool de stockage cloud. Un message d'erreur apparaît si plusieurs parutions utilisant un pool de stockage cloud présentent des dates redondantes ou si plusieurs lignes du même placement utilisent un pool de stockage cloud.
- Vous pouvez stocker un objet dans un pool de stockage cloud en même temps que celui-ci sous forme de copies répliquées ou avec code d'effacement dans StorageGRID. Toutefois, vous devez inclure plusieurs lignes dans l'instruction de placement pour la période, afin de pouvoir spécifier le nombre et les types de copies pour chaque emplacement.

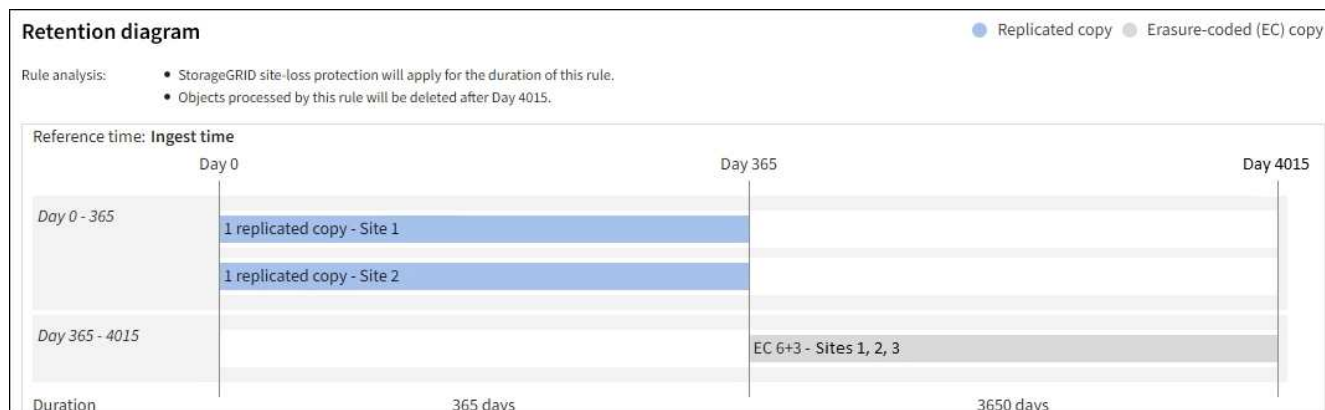
7. Dans le diagramme de conservation, confirmez vos instructions de placement.

Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une copie répliquée sur le site 2 pour la première année. Au bout d'un an et pendant 10 ans supplémentaires, une copie avec code d'effacement 6+3 sera sauvegardée sur trois sites. Au bout de 11 ans au total, les objets seront supprimés de StorageGRID.

La section analyse des règles du diagramme de rétention indique :

- La protection contre la perte de site StorageGRID s'appliquera pendant toute la durée de cette règle.
- Les objets traités par cette règle seront supprimés après le jour 4015.

Reportez-vous à ["Activer la protection contre la perte de site."](#)



8. Sélectionnez **Continuer**. ["Étape 3 \(Sélectionner le comportement d'ingestion\)"](#) De l'assistant de création d'une règle ILM s'affiche.

Utiliser le temps d'accès dans les règles ILM de StorageGRID

Vous pouvez utiliser l'heure du dernier accès comme heure de référence dans une règle ILM. Il peut par exemple être nécessaire de conserver les objets qui ont été affichés au cours des trois derniers mois sur les nœuds de stockage locaux tout en déplaçant des objets qui n'ont pas été considérés comme récemment vers un emplacement hors site. Vous pouvez également utiliser l'heure du dernier accès en tant que filtre avancé si vous souhaitez qu'une règle ILM s'applique uniquement aux objets auxquels vous avez accédé pour la dernière fois à une date spécifique.

Description de la tâche

Avant d'utiliser l'heure du dernier accès dans une règle ILM, consultez les considérations suivantes :

- Lorsque vous utilisez l'heure du dernier accès comme heure de référence, sachez que la modification de l'heure du dernier accès d'un objet ne déclenche pas une évaluation ILM immédiate. Les placements de l'objet sont alors évalués et l'objet est déplacé selon les besoins lors de l'évaluation de l'objet par la ILM en arrière-plan. L'accès à l'objet peut prendre deux semaines ou plus.

Prenez en compte cette latence lors de la création de règles ILM basées sur l'heure du dernier accès et évitez les placements qui utilisent des périodes courtes (moins d'un mois).

- Lorsque vous utilisez l'heure du dernier accès comme filtre avancé ou comme heure de référence, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3. Vous pouvez utiliser le ["Gestionnaire de locataires"](#) ou le ["API de gestion des locataires"](#).



Les mises à jour des heures du dernier accès sont désactivées par défaut pour les compartiments S3.



Notez qu'en activant les mises à jour du dernier accès, vous pouvez réduire les performances, en particulier dans les systèmes dotés d'objets de petite taille. L'impact sur les performances a lieu, car StorageGRID doit mettre à jour les objets avec un nouvel horodatage chaque fois que les objets sont récupérés.

Le tableau suivant indique si l'heure du dernier accès est mise à jour pour tous les objets du compartiment pour différents types de demandes.

Type de demande	Indique si l'heure du dernier accès est mise à jour lorsque les mises à jour de l'heure du dernier accès sont désactivées	Indique si l'heure du dernier accès est mise à jour lorsque les mises à jour de l'heure du dernier accès sont activées
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Oui
Demande de mise à jour des métadonnées d'un objet	Oui	Oui
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Sélectionnez le comportement d'ingestion pour une règle ILM StorageGRID

L'étape **Sélectionner le comportement d'ingestion** de l'assistant Créer une règle ILM vous permet de choisir la façon dont les objets filtrés par cette règle sont protégés lors de leur ingestion.

Description de la tâche

StorageGRID peut effectuer des copies intermédiaires et mettre en file d'attente les objets pour l'évaluation ILM, ou effectuer des copies pour répondre immédiatement aux instructions de placement de la règle.

Étapes

1. Sélectionnez le "[comportement d'ingestion](#)" à utiliser.

Pour plus d'informations, voir "[Avantages, inconvénients et limites des options d'acquisition](#)".

Vous ne pouvez pas utiliser l'option équilibrée ou stricte si la règle utilise l'un des placements suivants :



- Un pool de stockage cloud dès le premier jour
- Un 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 règles ILM pour un comportement d'ingestion strict](#)".

2. Sélectionnez **Créer**.

La règle ILM est créée. La règle ne devient active que si elle est ajoutée à un et que "[Politique ILM](#)" cette stratégie est activée.

Pour afficher les détails de la règle, sélectionnez son nom sur la page règles ILM.

Créez une règle ILM par défaut dans StorageGRID

Avant de créer une règle ILM, vous devez créer une règle par défaut afin de placer tous les objets qui ne correspondent pas à une autre règle de la politique. La règle par défaut ne peut pas utiliser de filtres. Elle doit s'appliquer à tous les locataires, à tous les compartiments et à toutes les versions d'objet.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Description de la tâche

La règle par défaut est la dernière règle évaluée dans une politique ILM. Elle ne peut donc pas utiliser de filtres. Les instructions de placement de la règle par défaut sont appliquées à tous les objets qui ne sont pas associés par une autre règle de la règle.

Dans cet exemple de règle, la première règle s'applique uniquement aux objets appartenant à test-tenant-1. La règle par défaut, qui est la dernière, s'applique aux objets appartenant à tous les autres comptes de tenant.

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'ajoutez à une stratégie.
- La règle par défaut ne peut pas utiliser de filtres de base ou avancés.
- La règle par défaut doit s'appliquer à toutes les versions d'objet.
- La règle par défaut doit créer des copies répliquées.



N'utilisez pas de règle qui crée des copies avec code d'effacement comme règle par défaut d'une règle. Les règles de code d'effacement doivent utiliser un filtre avancé pour empêcher le codage d'effacement des objets de petite taille.

- En général, la règle par défaut doit conserver les objets à tout jamais.
- Si vous utilisez (ou que vous prévoyez d'activer) le paramètre de verrouillage d'objet S3 global, la règle par défaut doit être conforme.

Étapes

1. Sélectionnez **ILM > règles**.
2. Sélectionnez **Créer**.

L'étape 1 (entrer les détails) de l'assistant de création de règle ILM s'affiche.

3. Entrez un nom unique pour la règle dans le champ **Nom de la règle**.
4. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.
5. Laissez le champ **tenant accounts** vide.

La règle par défaut doit s'appliquer à tous les comptes de tenant.

6. Laissez la liste déroulante Nom du compartiment comme **s'applique à tous les compartiments**.

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 aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée) ?"

8. N'ajoutez pas de filtres avancés.

La règle par défaut ne peut pas spécifier de filtres.

9. Sélectionnez **Suivant**.

L'étape 2 (définir les placements) s'affiche.

10. Pour heure de référence, sélectionnez une option.

Si vous avez conservé la réponse par défaut, **non**, pour la question, "appliquer cette règle aux anciennes versions d'objet uniquement?" L'heure non actuelle ne sera pas incluse dans la liste déroulante. La règle par défaut doit appliquer toutes les versions d'objet.

11. Spécifiez les instructions de placement pour la règle par défaut.

- La règle par défaut doit conserver les objets à tout jamais. Un avertissement s'affiche lorsque vous activez une nouvelle stratégie si la règle par défaut ne conserve pas les objets indéfiniment. Vous devez confirmer que c'est le comportement que vous attendez.
- La règle par défaut doit créer des copies répliquées.



N'utilisez pas de règle qui crée des copies avec code d'effacement comme règle par défaut d'une règle. Les règles de code d'effacement doivent inclure le filtre avancé **taille de l'objet (Mo) supérieure à 200 Ko** pour empêcher le codage d'effacement des objets plus petits.

- Si vous utilisez (ou si vous avez l'intention d'activer) le paramètre global de verrouillage d'objet S3, la règle par défaut doit être conforme :
 - Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
 - Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
 - Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
 - 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 « toujours ».

12. Consultez le diagramme de conservation pour confirmer vos instructions de placement.

13. Sélectionnez **Continuer**.

L'étape 3 (Sélectionner le comportement d'ingestion) s'affiche.

14. Sélectionnez l'option d'acquisition à utiliser, puis sélectionnez **Créer**.

Gestion des règles ILM

Découvrez les politiques ILM dans StorageGRID

Une règle de gestion du cycle de vie des informations (ILM) est un ensemble ordonné de règles ILM qui détermine la façon dont le système StorageGRID gère les données d'objet au fil du temps.



Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Règle ILM par défaut

Lorsque vous installez StorageGRID et ajoutez des sites, une politique ILM par défaut est automatiquement créée, comme suit :

- Si votre grille contient un site, la stratégie par défaut contient une règle par défaut qui réplique deux copies de chaque objet sur ce site.
- Si votre grille contient plusieurs sites, la règle par défaut réplique une copie de chaque objet sur chaque site.

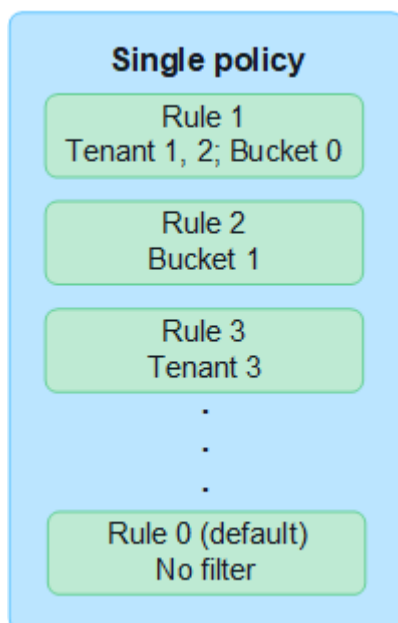
Si la politique par défaut ne répond pas à vos besoins de stockage, vous pouvez créer vos propres règles et politiques. Voir "[Création d'une règle ILM](#)" et "[Créer une règle ILM](#)".

Une ou plusieurs règles ILM actives ?

Vous pouvez avoir une ou plusieurs règles ILM actives à la fois.

Une politique

Si votre grid utilise un schéma de protection des données simple avec peu de règles spécifiques au locataire et au compartiment, utilisez une règle ILM active unique. Les règles ILM peuvent contenir des filtres pour gérer différents compartiments ou locataires.



Lorsque vous ne modifiez qu'une règle et que les exigences d'un locataire changent, vous devez créer une nouvelle règle ILM ou cloner la règle existante pour appliquer les modifications, simuler, puis activer la nouvelle règle ILM. Toute modification de la règle ILM peut entraîner des déplacements d'objets pouvant prendre plusieurs jours et entraîner une latence du système.

Plusieurs règles

Pour offrir différentes options de qualité de service aux locataires, vous pouvez avoir plusieurs règles actives à la fois. Chaque règle peut gérer des locataires, des compartiments S3 et des objets spécifiques. Lorsque vous appliquez ou modifiez une règle pour un ensemble spécifique de locataires ou d'objets, les règles appliquées aux autres locataires et objets ne sont pas affectées.

Balises de règles ILM

Si vous souhaitez permettre aux locataires de basculer facilement entre plusieurs règles de protection des données par compartiment, utilisez plusieurs règles ILM avec *ILM policy tags*. Vous attribuez chaque règle ILM à une balise, puis les locataires étiquettent un compartiment pour appliquer la règle à ce compartiment. Vous pouvez définir des balises de règles ILM sur des compartiments S3 uniquement.

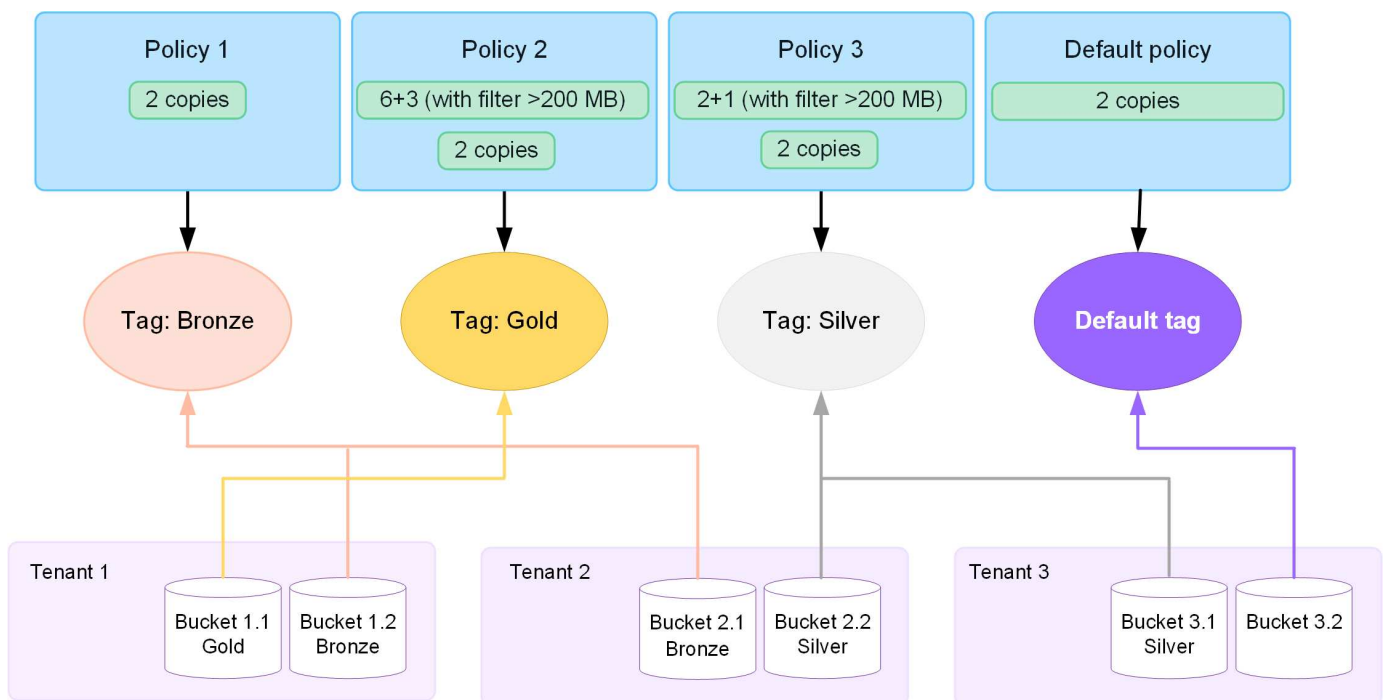
Par exemple, vous pouvez avoir trois étiquettes nommées Gold, Silver et Bronze. Vous pouvez attribuer une règle ILM à chaque balise, en fonction de la durée et de l'emplacement où cette règle stocke les objets. Les locataires peuvent choisir la règle à utiliser en étiquetant leurs compartiments. Un compartiment marqué Gold est géré par la politique Gold et reçoit le niveau Gold de protection des données et de performances.



Tu peux "créer un maximum de 10 balises de stratégie" pour votre grille.

Balise de règle ILM par défaut

Une balise de règle ILM par défaut est automatiquement créée lors de l'installation de StorageGRID. Chaque grille doit avoir une règle active affectée à la balise par défaut. La règle par défaut s'applique à tous les compartiments S3 non balisés.



Comment une règle ILM évalue-t-elle les objets ?

Une règle ILM active permet de contrôler le placement, la durée et la protection des données des objets.

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

1. Si les filtres de la première règle de la règle correspondent à un objet, celui-ci est ingéré conformément au comportement d'ingestion de cette règle et stocké conformément aux instructions de placement de cette règle.
2. Si les filtres de la première règle ne correspondent pas à l'objet, l'objet est évalué par rapport à chaque règle ultérieure de la règle jusqu'à ce qu'une correspondance soit établie.
3. Si aucune règle ne correspond à un objet, les instructions de comportement d'ingestion et de placement de la règle par défaut de cette règle sont appliquées. La règle par défaut est la dernière règle d'une stratégie. La règle par défaut doit s'appliquer à tous les locataires, à tous les compartiments S3 et à toutes les versions d'objet. Elle ne peut pas utiliser de filtres avancés.

Exemple de règle ILM

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

• Règle 1 : copies répliquées pour le locataire A

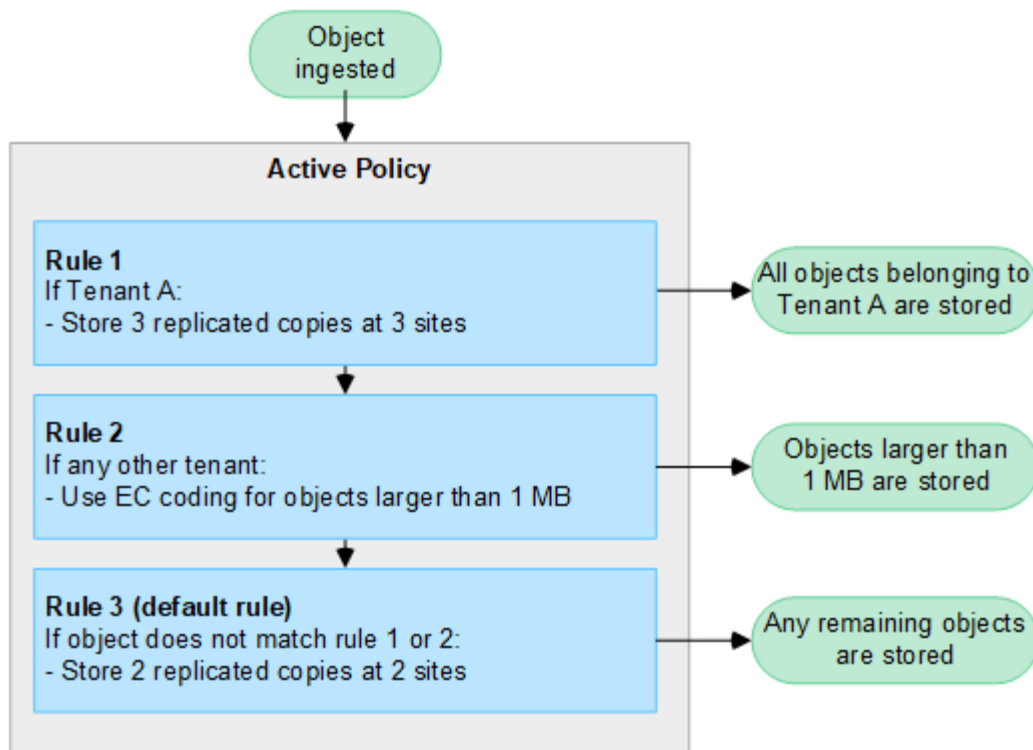
- Faites correspondre tous les objets appartenant au locataire A.
- Stockez ces objets sous forme de trois copies répliquées sur trois sites.
- Les objets appartenant à d'autres locataires ne correspondent pas à la règle 1, ils sont donc évalués par rapport à la règle 2.

• Règle 2 : code d'effacement pour les objets supérieurs à 1 Mo

- Faites correspondre tous les objets d'autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus volumineux sont stockés au moyen d'un code d'effacement de 6+3 sur trois sites.
- Ne correspond pas aux objets de 1 Mo ou moins, ces objets sont donc évalués par rapport à la règle 3.

• Règle 3 : 2 copies 2 centres de données (par défaut)

- Est la dernière règle et la règle par défaut de la règle. N'utilise pas de filtres.
- Faites deux copies répliquées de tous les objets qui ne correspondent pas à la règle 1 ou à la règle 2 (objets qui n'appartiennent pas au locataire A de 1 Mo ou moins).



Que sont les stratégies actives et inactives ?

Chaque système StorageGRID doit disposer d'au moins une règle ILM active. Si vous souhaitez avoir plusieurs règles ILM actives, vous créez des balises de règles ILM et vous affectez une règle à chaque balise. Les locataires appliquent ensuite des balises aux compartiments S3. La règle par défaut s'applique à tous les objets des compartiments auxquels aucune balise de règle n'est attribuée.

Lorsque vous créez une règle ILM pour la première fois, vous sélectionnez une ou plusieurs règles ILM et vous les organisez dans un ordre spécifique. Après avoir simulé la stratégie pour confirmer son comportement, vous l'activez.

Lorsque vous activez une règle ILM, StorageGRID utilise cette règle 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 règle sont mises en œuvre.

Si vous activez plusieurs règles ILM à la fois et que les locataires appliquent des balises de règles à des compartiments S3, les objets de chaque compartiment sont gérés en fonction de la règle attribuée à la balise.

Un système StorageGRID suit l'historique des stratégies qui ont été activées ou désactivées.

Facteurs à prendre en compte lors de la création d'une règle ILM

- Utilisez uniquement la règle de base 2 copies fournie par le système dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle Make 2 copies de cette règle utilise le pool de stockage All Storage Nodes, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.



Le pool de stockage tous les nœuds de stockage est automatiquement créé lors de l'installation de StorageGRID 11.6 et des versions antérieures. Si vous effectuez une mise à niveau vers une version ultérieure de StorageGRID, le pool tous les nœuds de stockage existera toujours. Si vous installez StorageGRID 11.7 ou une version ultérieure en tant que nouvelle installation, le pool tous les nœuds de stockage n'est pas créé.

- Lors de la conception d'une nouvelle politique, tenez compte de tous les différents types d'objets pouvant être ingérés dans votre grille. Assurez-vous que la stratégie inclut des règles pour correspondre et placer ces objets selon les besoins.
- Privilégiez la simplicité des règles ILM. Cela permet d'éviter les situations dangereuses dans lesquelles les données d'objet ne sont pas protégées comme prévu lorsque des modifications sont apportées au système StorageGRID au fil du temps.
- Assurez-vous que les règles de la police sont dans le bon ordre. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut. Par exemple, si la première règle d'une règle correspond à un objet, cet objet ne sera évalué par aucune autre règle.
- La dernière règle de chaque politique ILM est la règle ILM par défaut, qui ne peut utiliser aucun filtre. Si un objet n'a pas été mis en correspondance par une autre règle, la règle par défaut contrôle l'emplacement de cet objet et la durée de conservation.
- Avant d'activer une nouvelle stratégie, vérifiez les modifications apportées par la stratégie au placement des objets existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Créer des règles ILM dans StorageGRID

Créez une ou plusieurs règles ILM pour répondre à vos exigences en matière de qualité de service.

Une règle ILM active vous permet d'appliquer les mêmes règles ILM à tous les locataires et compartiments.

L'utilisation de plusieurs règles ILM actives vous permet d'appliquer les règles ILM à des locataires et des compartiments spécifiques pour satisfaire à plusieurs exigences de qualité de service.

Créer une règle ILM

Description de la tâche

Avant de créer votre propre stratégie, vérifiez que le ["Règle ILM par défaut"](#) ne répond pas à vos besoins en stockage.



Utilisez uniquement les stratégies fournies par le système, la règle de 2 copies (pour les grilles à un site) ou une copie par site (pour les grilles à plusieurs sites), dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle par défaut de cette règle utilise le pool de stockage tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.



Si ["Le paramètre de verrouillage d'objet S3 global a été activé"](#), vous devez vous assurer que la stratégie ILM est conforme aux exigences des compartiments pour lesquels le verrouillage d'objets S3 est activé. Dans cette section, suivez les instructions qui mentionnent l'activation du verrouillage d'objets S3.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).
- Vous avez ["Création de règles ILM"](#) déterminé si le verrouillage objet S3 est activé ou non.

Verrouillage objet S3 non activé

- Vous ["Création des règles ILM"](#) souhaitez ajouter à la stratégie. Si nécessaire, vous pouvez enregistrer une stratégie, créer des règles supplémentaires, puis modifier la stratégie pour ajouter les nouvelles règles.
- Vous avez ["Une règle ILM par défaut a été créée"](#) qui ne contient aucun filtre.

Verrouillage objet S3 activé

- Le ["Le paramètre de verrouillage d'objet S3 global est déjà activé"](#) pour le système StorageGRID.
- Vous ["Vous avez créé des règles ILM conformes et non conformes"](#) souhaitez ajouter à la stratégie. Si nécessaire, vous pouvez enregistrer une stratégie, créer des règles supplémentaires, puis modifier la stratégie pour ajouter les nouvelles règles.
- Vous avez ["Une règle ILM par défaut a été créée"](#) pour la politique qui est conforme.

- En option, vous avez regardé la vidéo :

Aperçu des politiques ILM

Voir aussi ["Règles ILM"](#).

Étapes

1. Sélectionnez **ILM > stratégies**.

Si le paramètre global S3 Object Lock est activé, la page des règles ILM indique les règles ILM compatibles.

2. Détermination de la méthode de création de la règle ILM

Création de la règle

- a. Sélectionnez **Créer une stratégie**.

Cloner la règle existante

- a. Cochez la case correspondant à la stratégie que vous souhaitez utiliser, puis sélectionnez **Clone**.

Modifier une stratégie existante

- a. Si une stratégie est inactive, vous pouvez la modifier. Cochez la case correspondant à la stratégie inactive que vous souhaitez utiliser, puis sélectionnez **Modifier**.

3. Dans le champ **Policy name**, entrez un nom unique pour la stratégie.
4. Si vous le souhaitez, dans le champ **motif du changement**, entrez la raison pour laquelle vous créez une nouvelle stratégie.
5. Pour ajouter des règles à la stratégie, sélectionnez **Sélectionner des règles**. Sélectionnez un nom de règle pour afficher les paramètres de cette règle.

Si vous clonez une règle :

- Vous sélectionnez les règles utilisées par la règle de clonage.
- Si la stratégie que vous utilisez est une règle sans filtre qui n'était pas la règle par défaut, vous êtes invité à supprimer toutes ces règles, sauf une.
- Si la règle par défaut utilise un filtre, vous êtes invité à sélectionner une nouvelle règle par défaut.
- Si la règle par défaut n'était pas la dernière, vous pouvez la déplacer vers la fin de la nouvelle règle.

Verrouillage objet S3 non activé

- a. Sélectionnez une règle par défaut pour la stratégie. Pour créer une nouvelle règle par défaut, sélectionnez **page règles ILM**.

La règle par défaut s'applique aux objets qui ne correspondent pas à une autre règle de la stratégie. La règle par défaut ne peut pas utiliser de filtres et est toujours évaluée en dernier.



N'utilisez pas la règle Make 2 copies comme règle par défaut pour une stratégie. La règle Make 2 copies utilise un pool de stockage unique, tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.

Verrouillage objet S3 activé

- a. Sélectionnez une règle par défaut pour la stratégie. Pour créer une nouvelle règle par défaut, sélectionnez **page règles ILM**.

La liste des règles contient uniquement les règles qui sont conformes et n'utilisent aucun filtre.



N'utilisez pas la règle Make 2 copies comme règle par défaut pour une stratégie. La règle Make 2 copies utilise un pool de stockage unique, tous les nœuds de stockage, qui contient tous les sites. Si vous utilisez cette règle, plusieurs copies d'un objet peuvent être placées sur le même site.

- b. Si vous avez besoin d'une règle « par défaut » différente pour les objets dans des compartiments S3 non conformes, sélectionnez **inclure une règle sans filtres pour les compartiments S3 non conformes**, et sélectionnez une règle non conforme qui n'utilise pas de filtre.

Par exemple, vous pouvez utiliser un pool de stockage cloud pour stocker des objets dans des compartiments pour lesquels le verrouillage d'objet S3 n'est pas activé.



Vous ne pouvez sélectionner qu'une règle non conforme qui n'utilise pas de filtre.

Voir aussi ["Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3"](#).

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 stratégie. Ces règles utilisent au moins un filtre (compte de locataire, nom de compartiment, filtre avancé ou heure de référence non courante). Sélectionnez ensuite **Sélectionner**.

La fenêtre Créer une stratégie répertorie à présent les règles que vous avez sélectionnées. La règle par

défaut est à la fin, avec les autres règles au-dessus.

Si le verrouillage d'objet S3 est activé et que vous avez également sélectionné une règle « par défaut » non conforme, cette règle est ajoutée en tant que règle de second à dernier dans la stratégie.



Un avertissement s'affiche si une règle ne conserve pas les objets indéfiniment. Lorsque vous activez cette règle, vous devez confirmer que vous souhaitez que StorageGRID supprime des objets lorsque les instructions de placement pour la règle par défaut s'affichent (à moins qu'un cycle de vie de compartiment ne conserve les objets pendant une période plus longue).

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 une règle a été sélectionnée.



Vous devez confirmer que les règles ILM sont dans l'ordre correct. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut.

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 règles ILM supplémentaires.
12. [Simulation d'une règle ILM](#). Vous devez toujours simuler une stratégie avant de l'activer pour vous assurer qu'elle fonctionne comme prévu.

Simuler une règle

Simulez une stratégie sur des objets test avant d'activer la stratégie et de l'appliquer à vos données de production.

Avant de commencer

Vous connaissez le compartiment S3/clé-objet pour chaque objet à tester.

Étapes

1. À l'aide d'un client S3 ou du ["Console S3"](#), ingérer les objets requis pour tester chaque règle.
2. Sur la page règles ILM, cochez la case correspondant à la règle, puis sélectionnez **Simulate**.
3. Dans le champ **Object**, entrez S3 bucket/object-key pour un objet test. Par exemple bucket-01/filename.png, .
4. Si la gestion des versions S3 est activée, entrez éventuellement un ID de version pour l'objet dans le champ **ID de version**.
5. Sélectionnez **simuler**.
6. Dans la section Résultats de simulation, vérifiez que chaque objet a été mis en correspondance avec la règle correcte.
7. Pour déterminer quel pool de stockage ou profil de code d'effacement est en vigueur, sélectionnez le nom de la règle correspondante pour accéder à la page de détails de la règle.



Vérifiez toutes les modifications apportées au placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Résultats

Toute modification apportée aux règles de la stratégie sera prise en compte dans les résultats de la simulation et affichera la nouvelle correspondance ainsi que la correspondance précédente. La fenêtre de simulation de stratégie conserve les objets testés jusqu'à ce que vous sélectionniez **Tout effacer** ou l'icône de suppression  pour chaque objet dans la liste des résultats de la simulation.

Informations associées

["Exemples de simulations de règles ILM"](#)

Activer une stratégie

Lorsque vous activez une seule nouvelle règle ILM, les objets existants et les nouveaux objets ingérés sont gérés par cette règle. Lorsque vous activez plusieurs règles, les balises de règles ILM attribuées aux compartiments déterminent les objets à gérer.

Avant d'activer une nouvelle stratégie :

1. Simulez la règle pour confirmer qu'elle se comporte comme vous l'attendez.
2. Vérifiez toutes les modifications apportées au placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.



Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables.

Description de la tâche

Lorsque vous activez une règle ILM, le système distribue la nouvelle règle à tous les nœuds. Cependant, la nouvelle règle active peut ne pas être appliquée tant que tous les nœuds du grid ne sont pas disponibles pour recevoir la nouvelle règle. Dans certains cas, le système attend d'implémenter une nouvelle stratégie active pour s'assurer que les objets de grille ne sont pas accidentellement supprimés. Détails :

- Si vous apportez des modifications de stratégie qui **augmentent la redondance ou la durabilité des données**, ces modifications sont mises en œuvre immédiatement. Par exemple, si vous activez une nouvelle règle incluant une règle à trois copies au lieu d'une règle à deux copies, cette règle sera immédiatement implémentée car elle accroît la redondance des données.
- Si vous apportez des modifications de stratégie qui **pourraient réduire la redondance ou la durabilité des données**, ces modifications ne seront pas implémentées tant que tous les nœuds de grille ne seront pas disponibles. Par exemple, si vous activez une nouvelle stratégie qui utilise une règle à deux copies au lieu d'une règle à trois copies, la nouvelle stratégie s'affiche dans l'onglet Stratégie active, mais elle ne prend effet que lorsque tous les nœuds sont en ligne et disponibles.

Étapes

Pour activer une ou plusieurs stratégies, procédez comme suit :

Activez une stratégie

Procédez comme suit si vous n'avez qu'une seule stratégie active. Si vous avez déjà une ou plusieurs stratégies actives et que vous activez d'autres stratégies, suivez les étapes d'activation de plusieurs stratégies.

1. Lorsque vous êtes prêt à activer une stratégie, sélectionnez **ILM > Politiques**.

Vous pouvez également activer une seule stratégie à partir de la page **ILM > balises de stratégie**.

2. Dans l'onglet stratégies, cochez la case correspondant à la stratégie que vous souhaitez activer, puis sélectionnez **Activer**.
3. Suivez l'étape appropriée :
 - Si un message d'avertissement vous invite à confirmer l'activation de la stratégie, sélectionnez **OK**.
 - Si un message d'avertissement contenant des détails sur la police s'affiche :
 - i. Examinez les détails pour vous assurer que la règle gérerait les données comme prévu.
 - ii. Si la règle par défaut stocke des 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 indéfiniment, mais qu'une ou plusieurs autres règles ont une rétention limitée, tapez **yes** dans la zone de texte.
 - iv. Sélectionnez **Activer la stratégie**.

Activez plusieurs règles

Pour activer plusieurs stratégies, vous devez créer des balises de stratégie et attribuer une stratégie à chaque balise. Vous pouvez créer un maximum de 10 balises de stratégie pour votre grille.



Lorsque plusieurs balises de stratégie sont utilisées, si les locataires réaffectent fréquemment les balises de stratégie aux buckets, les performances de la grille peuvent être affectées. Si vous avez des locataires non approuvés, envisagez d'utiliser uniquement la balise de stratégie par défaut.

1. Sélectionnez **ILM > balises de stratégie**.
2. Sélectionnez **Créer**.
3. Dans la boîte de dialogue Créer une balise de stratégie, saisissez un nom de balise et, éventuellement, une description de la balise.



Les noms et les descriptions des étiquettes sont visibles pour les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de règles à affecter à leurs compartiments. Par exemple, si la règle attribuée supprime des objets après un certain temps, vous pouvez l'indiquer dans la description. N'incluez pas d'informations sensibles dans ces champs.

4. Sélectionnez **Créer une balise**.
5. Dans le tableau des balises de règles ILM, utilisez la liste déroulante pour sélectionner une règle à attribuer à la balise.
6. Si des avertissements apparaissent dans la colonne restrictions de la stratégie, sélectionnez **Afficher les détails de la stratégie** pour examiner la stratégie.

7. Assurez-vous que chaque règle gèrerait les données comme prévu.
8. Sélectionnez **Activer les stratégies attribuées**. Vous pouvez également sélectionner **Effacer les modifications** pour supprimer l'affectation de police.
9. Dans la boîte de dialogue Activer les stratégies avec de nouvelles balises, consultez les descriptions de la façon dont chaque balise, règle et règle gèrera les objets. Apportez les modifications nécessaires pour vous assurer que les règles gèreront les objets comme prévu.
10. Lorsque vous êtes sûr de vouloir activer les stratégies, tapez **oui** dans la zone de texte, puis sélectionnez **Activer les stratégies**.

Informations associées

"Exemple 6 : modification d'une règle ILM"

Exemples de simulations de stratégies ILM dans StorageGRID

Les exemples de simulations de règles ILM fournissent des instructions pour structurer et modifier des simulations pour votre environnement.

Exemple 1 : vérification des règles lors de la simulation d'une règle ILM

Cet exemple décrit comment vérifier des règles lors de la simulation d'une stratégie.

Dans cet exemple, la **exemple de règle ILM** est simulée contre les objets ingérés dans deux compartiments. La politique comprend trois règles, comme suit :

- La première règle, **deux copies, deux ans pour le compartiment a**, ne s'applique qu'aux objets du compartiment a.
- La deuxième règle, **objets EC > 1 Mo**, s'applique à tous les compartiments, mais aux filtres sur des objets supérieurs à 1 Mo.
- La troisième règle, **deux copies, deux centres de données**, est la règle par défaut. Il n'inclut aucun filtre et n'utilise pas l'heure de référence non actuelle.

Après avoir simulé la règle, confirmez que chaque objet a été mis en correspondance avec la règle appropriée.

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	—	X
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	X
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	X

Dans cet exemple :

- `bucket-a/bucket-a object.pdf` correspond correctement à la première règle, qui filtre les objets dans `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` est dans `bucket-b`, donc il ne correspond pas à la première règle. Au lieu de cela, il a été correctement mis en correspondance par la deuxième règle, qui filtre les objets de plus de 1 Mo.
- `bucket-b/test object less than 1 MB.pdf` ne correspondant pas aux filtres des deux premières règles, il sera donc placé par la règle par défaut, qui n'inclut pas de filtres.

Exemple 2 : réorganisation des règles lors de la simulation d'une politique ILM

Cet exemple montre comment vous pouvez réorganiser les règles pour modifier les résultats lors de la simulation d'une règle.

Dans cet exemple, la politique **Demo** est en cours de simulation. Cette règle, qui vise à trouver des objets qui ont des métadonnées utilisateur `série=x-men`, comprend trois règles, comme suit :

- La première règle, **PNgs**, filtre les noms de clés qui se terminent par `.png`.
- La deuxième règle, **X-MEN**, ne s'applique qu'aux objets pour tenant A et aux filtres pour les `series=x-men` métadonnées utilisateur.
- La dernière règle, **deux copies deux centres de données**, est la règle par défaut, qui correspond à tous les objets qui ne correspondent pas aux deux premières règles.

Étapes

1. Après avoir ajouté les règles et enregistré la stratégie, sélectionnez **Simulate**.
2. Dans le champ **Object**, entrez le compartiment S3/clé-objet pour un objet test et sélectionnez **Simulate**.

Les résultats de la simulation s'affichent, indiquant que l'`Havok.png` objet a été mis en correspondance avec 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 destiné à tester la règle **X-MEN**.

3. Pour résoudre le problème, réorganisez les règles.
 - a. Sélectionnez **Terminer** pour fermer la fenêtre simuler une politique ILM.
 - b. Sélectionnez **Modifier** pour modifier la stratégie.
 - c. Faites glisser la règle **X-men** en haut de la liste.
 - d. Sélectionnez **Enregistrer**.
4. Sélectionnez **simuler**.

Les objets que vous avez testés précédemment sont réévalués par rapport à la règle mise à jour et les

nouveaux résultats de simulation sont affichés. Dans l'exemple, la colonne correspondance de règle indique que l' `Havok.png` objet correspond désormais à la règle de métadonnées X-MEN, comme prévu. La colonne comparaison précédente indique que la règle des 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	✕

Exemple 3 : correction d’une règle lors de la simulation d’une règle ILM

Cet exemple montre comment simuler une stratégie, corriger une règle dans la règle et poursuivre la simulation.

Dans cet exemple, la politique **Demo** est en cours de simulation. Cette règle a pour but de rechercher des objets qui ont des `series=x-men` métadonnées utilisateur. Cependant, des résultats inattendus se sont produits lors de la simulation de cette règle par rapport à l' `Beast.jpg` objet. Au lieu de faire correspondre la règle de métadonnées X-Men, l'objet correspond à la règle par défaut, deux copies de deux centres de données.

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	—	✕

Lorsqu'un objet test n'est pas associé à la règle attendue de la stratégie, vous devez examiner chaque règle de la stratégie et corriger les erreurs éventuelles.

Étapes

- Sélectionnez **Terminer** pour fermer la boîte de dialogue simuler la stratégie. Sur la page de détails de la stratégie, sélectionnez **diagramme de rétention**. Sélectionnez ensuite **développer tout** ou **Afficher les détails** pour chaque règle selon les besoins.
- Vérifiez le compte de locataire de la règle, l'heure de référence et les critères de filtrage.

Supposons, par exemple, que les métadonnées de la règle X-MEN aient été saisies comme "x-men01" au lieu de "X-MEN".

- Pour résoudre l'erreur, corrigez la règle comme suit :
 - Si la règle fait partie de la règle, vous pouvez la cloner ou la supprimer de la règle, puis la modifier.
 - Si la règle fait partie de la stratégie active, vous devez cloner la règle. Vous ne pouvez pas modifier ou supprimer une règle de la stratégie active.

4. Exécuter à nouveau la simulation.

Dans cet exemple, la règle X-MEN corrigée correspond désormais à l' `Beast.jpg` objet en fonction des `series=x-men` métadonnées de l'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 stratégie ILM dans StorageGRID

Vous pouvez afficher les détails des balises de règles ILM, modifier une balise ou supprimer une balise.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Afficher le détail des balises de règles ILM

Pour afficher les détails d'une étiquette :

1. Sélectionnez **ILM > balises de stratégie**.
2. Sélectionnez le nom de la stratégie dans la table. La page de détails de l'étiquette s'affiche.
3. Sur la page de détails, affichez l'historique précédent des stratégies attribuées.
4. Affichez une stratégie en la sélectionnant.

Modifiez la balise de règle ILM



Les noms et les descriptions des étiquettes sont visibles pour les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de règles à affecter à leurs compartiments. Par exemple, si la règle attribuée supprime des objets après un certain temps, vous pouvez l'indiquer 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 stratégie**.
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 s'affiche et vous pouvez sélectionner **Modifier** sur cette page.

3. Modifiez la description de la balise si nécessaire

4. Sélectionnez **Enregistrer**.

Suppression de la balise de règle ILM

Lorsque vous supprimez une balise de règle, la règle par défaut s'applique à tous les compartiments affectés à cette balise.

Pour supprimer une balise :

1. Sélectionnez **ILM > balises de stratégie**.
2. Cochez la case correspondant à la balise, puis sélectionnez **Supprimer**. Une boîte de dialogue de confirmation s'affiche.

Vous pouvez également sélectionner le nom de la balise. La page de détails de la balise s'affiche et vous pouvez sélectionner **Supprimer** sur cette page.

3. Sélectionnez **Oui** pour supprimer la balise.

Informations associées

["En savoir plus sur la création de balises de stratégie ILM"](#)

Vérifiez une stratégie ILM avec la recherche de métadonnées d'objet dans StorageGRID

Après avoir activé une règle ILM, vous ingérer des objets de test représentatifs dans le système StorageGRID, puis effectuer une recherche de métadonnées d'objet pour vérifier que les copies sont effectuées comme prévu et placées dans les emplacements appropriés.

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. Ingestion de l'objet.
2. Sélectionnez **ILM > Object metadata Lookup**.
3. Saisissez l'identifiant de l'objet dans le champ **Identificateur**. Vous pouvez entrer un UUID, CBID ou une clé compartiment/objet S3.
4. Si vous le souhaitez, entrez un ID de version pour l'objet (S3 uniquement).
5. Sélectionnez **rechercher**.

Les résultats de la recherche de métadonnées d'objet s'affichent. Cette page répertorie les types d'informations suivants :

- Métadonnées système, telles que l'ID 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 de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

6. Vérifiez que l'objet est stocké à l'emplacement correct et qu'il s'agit du bon type de copie.

Si l'option Audit est activée, vous pouvez également surveiller le journal d'audit du message règles objet respectées ORLM. Le message d'audit ORLM peut vous fournir davantage d'informations sur l'état du processus d'évaluation ILM, mais il ne peut pas vous fournir d'informations sur l'exactitude du placement des données de l'objet ou l'exhaustivité de la politique ILM. Vous devez évaluer cela vous-même. Pour plus de détails, voir ["Examiner les journaux d'audit"](#).

L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.



La capture d'écran suivante en est un exemple. Vos résultats varient 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": {
      "PAIS": "2",

```

Informations associées

["UTILISEZ L'API REST S3"](#)

Travaillez avec les règles ILM et les politiques ILM dans StorageGRID

À mesure que vos exigences de stockage évoluent, vous devrez peut-être mettre en place d'autres règles ou modifier les règles ILM associées à une règle. Vous pouvez consulter les metrics ILM pour déterminer les performances du système.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Afficher les règles ILM

Pour afficher les règles ILM actives et inactives et l'historique d'activation des règles :

1. Sélectionnez **ILM > stratégies**.
2. Sélectionnez **stratégies** pour afficher la liste des stratégies actives et inactives. Le tableau répertorie le nom de chaque stratégie, les balises auxquelles la stratégie est affectée et indique si la stratégie est active ou inactive.
3. Sélectionnez **Historique d'activation** pour afficher la liste des dates de début et de fin d'activation des polices.
4. Sélectionnez un nom de stratégie pour afficher les détails de la stratégie.



Si vous affichez les détails d'une police dont le statut est modifié ou supprimé, un message s'affiche pour vous expliquer que vous affichez la version de la stratégie qui était active pendant la période spécifiée et qui a depuis été modifiée ou supprimée.

Modification d'une règle ILM

Vous pouvez uniquement modifier une stratégie inactive. Si vous souhaitez modifier une règle active, désactivez-la ou créez un clone, puis modifiez le clone.

Pour modifier une stratégie :

1. Sélectionnez **ILM > stratégies**.
2. Cochez la case correspondant à la stratégie à modifier, puis sélectionnez **Modifier**.
3. Modifiez la stratégie en suivant les instructions de "[Création de règles ILM](#)" la section .
4. Simulez la stratégie avant de la réactiver.



Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Cloner une règle ILM

Pour cloner une règle ILM :

1. Sélectionnez **ILM > stratégies**.
2. Cochez la case correspondant à la stratégie à cloner, puis sélectionnez **Clone**.
3. Créez une nouvelle stratégie en commençant par la stratégie que vous avez clonée en suivant les instructions de la section "[Création de règles ILM](#)".



Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Suppression d'une règle ILM

La suppression d'une règle ILM est uniquement possible si elle est inactive. Pour supprimer une stratégie :

1. Sélectionnez **ILM > stratégies**.
2. Cochez la case correspondant à la stratégie inactive à supprimer.
3. Sélectionnez **Supprimer**.

Afficher le détail des règles ILM

Pour afficher les détails d'une règle ILM, y compris le diagramme de conservation et les instructions de placement de la règle :

1. Sélectionnez **ILM > règles**.
2. Sélectionnez le nom de la règle dont vous souhaitez afficher les détails. Exemple :

The screenshot shows the '2 copies 2 data centers' rule details page. At the top, it lists properties: Compliant: No, Ingest behavior: Strict, Reference time: Noncurrent time. Below these are buttons for Clone, Edit, and Remove. A tabbed interface shows 'Rule detail' (active) and 'Used in policies'. The 'Time period and placements' section has two tabs: 'Retention diagram' (active) and 'Placement instructions'. Under 'Retention diagram', there are buttons for 'Sort placements by' (Time period, Storage pool) and a legend for 'Replicated copy' (blue dot) and 'Erasure-coded (EC) copy' (grey dot). The 'Rule analysis' section states: 'Objects processed by this rule will not be deleted by ILM.' The main part of the diagram shows a timeline from 'Day 0' to 'Forever'. It displays two placement instructions: '2 replicated copies - Data Center 1' (blue bar) and 'EC 2+1 - Data Center 1' (grey bar). The x-axis is labeled 'Duration' and 'Forever'.

En outre, 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 stratégie.

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 règle, vous devez la cloner à la place et modifier le clone. Après avoir modifié le clone, vous pouvez supprimer la règle d'origine de la règle et la remplacer par la version modifiée si nécessaire.



Une règle ILM ne peut pas être clonée 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 à cloner, puis sélectionnez **Clone**. Vous pouvez également sélectionner le nom de la règle, puis sélectionner **Clone** dans la page des détails de la règle.
3. Mettez à jour la règle clonée en suivant les étapes pour [Modification d'une règle ILM](#) et [Utilisation de](#)

[filtres avancés dans les règles ILM](#)".

Lors du clonage d'une règle ILM, vous devez entrer un nouveau nom.

Modifiez une règle ILM

Vous devrez peut-être modifier une règle ILM pour modifier une instruction de filtre ou de placement.

Vous ne pouvez pas modifier une règle si elle est utilisée dans une règle ILM. Vous pouvez [cloner la règle](#) modifier la copie clonée et y apporter toutes les modifications nécessaires.



Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Étapes

1. Sélectionnez **ILM > règles**.
2. Vérifiez que la règle à modifier n'est utilisée dans aucune règle 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 de détails de la règle.
4. Suivez les étapes de l'assistant Modifier une règle ILM. Si nécessaire, suivez les étapes pour "[Création d'une règle ILM](#)" et "[Utilisation de filtres avancés dans les règles ILM](#)".

Lors de la modification d'une règle ILM, vous ne pouvez pas en modifier le nom.

Suppression d'une règle ILM

Pour gérer la liste des règles ILM actuelles, supprimez toutes les règles ILM que vous ne serez pas susceptible d'utiliser.

Étapes

Pour supprimer une règle ILM actuellement utilisée dans une policy active :

1. Cloner la règle.
2. Supprime la règle ILM du clone de règle.
3. Enregistrez, simulez et activez la nouvelle stratégie pour vous assurer que les objets sont protégés comme prévu.
4. Accédez à la procédure de suppression d'une règle ILM actuellement utilisée dans une stratégie inactive.

Pour supprimer une règle ILM actuellement utilisée dans une politique inactive :

1. Sélectionnez la stratégie inactive.
2. Supprimez la règle ILM de la règle ou [supprimez la stratégie](#).
3. Accédez à la procédure de suppression d'une règle ILM non utilisée actuellement.

Pour supprimer une règle ILM non utilisée actuellement :

1. Sélectionnez **ILM > règles**.

2. Confirmez que la règle que vous souhaitez supprimer n'est utilisée dans aucune stratégie.
3. Si la règle que vous souhaitez supprimer n'est pas utilisée, sélectionnez-la 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 metrics ILM

Vous pouvez afficher les mesures de la règle ILM, telles que le nombre d'objets dans la file d'attente et la fréquence d'évaluation. Vous pouvez surveiller ces mesures afin de déterminer les performances du système. Une file d'attente ou un taux d'évaluation important peut indiquer que le système ne peut pas suivre le taux d'entrée, que la charge des applications clientes est excessive ou qu'il existe une condition anormale.

Étapes

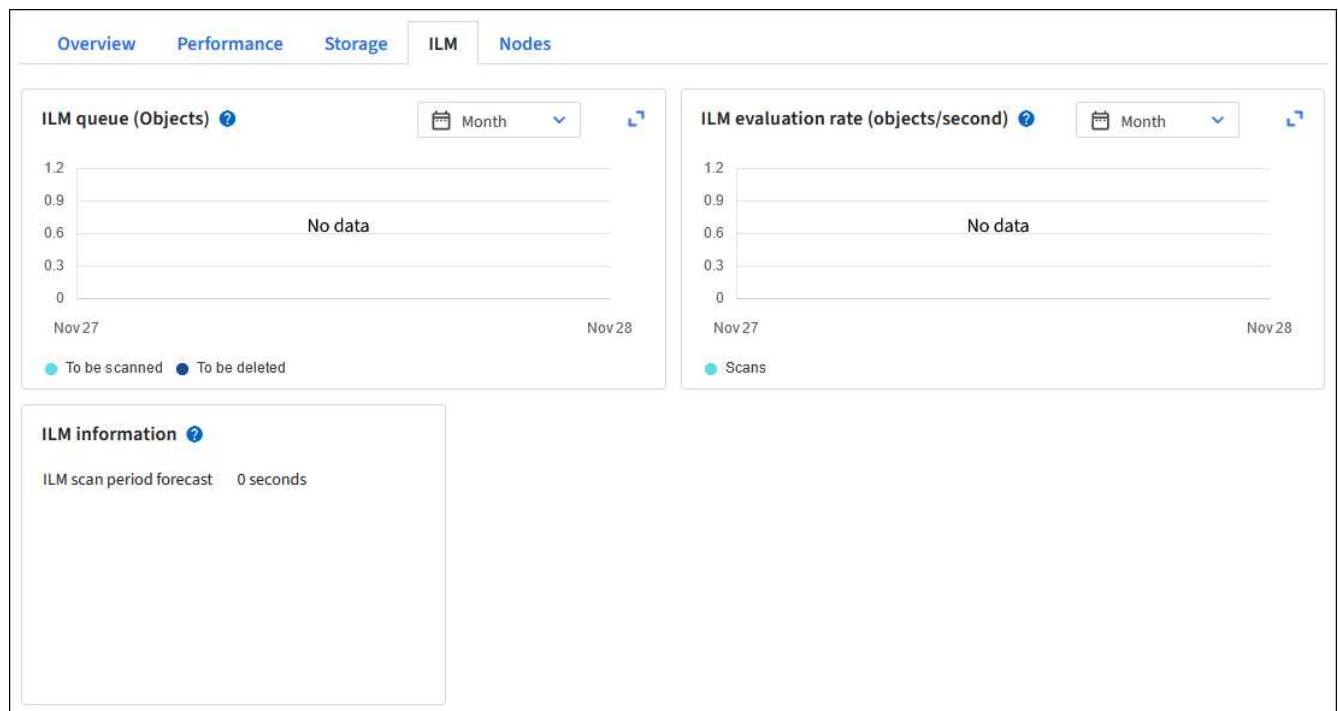
1. Sélectionnez **Tableau de bord > ILM**.



Le tableau de bord pouvant être personnalisé, l'onglet ILM peut ne pas être disponible.

2. Surveillez les mesures dans l'onglet ILM.

Vous pouvez sélectionner le point d'interrogation (?) pour afficher une description des éléments de l'onglet ILM.



Utilisez le verrouillage d'objet S3

Comment le verrouillage d'objets S3 protège les objets dans StorageGRID

En tant qu'administrateur du grid, vous pouvez activer le verrouillage objet S3 sur votre système StorageGRID et mettre en œuvre une règle ILM conforme pour empêcher la suppression ou l'écrasement des objets de compartiments S3 spécifiques pendant une

durée spécifiée.

Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objets S3 est activé pour un système StorageGRID, un compte locataire S3 peut créer des compartiments avec ou sans le verrouillage d'objets S3 activé. Lorsque l'option permettant d'autoriser le verrouillage d'objets S3 pour les compartiments existants est activée, un compte locataire S3 peut activer le verrouillage d'objets S3 pour un compartiment existant. Si un compartiment a le verrouillage d'objets S3 activé, le versionnage du compartiment est requis et est activé automatiquement. Après qu'un compte locataire S3 a activé le verrouillage d'objets S3 pour un compartiment nouveau ou existant, il ne peut plus être désactivé.

Un compartiment sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne possède de paramètres de conservation.

Un compartiment avec S3 Object Lock peut contenir des objets avec et sans paramètres de conservation spécifiés par les applications client S3. Certains objets ingérés auront des paramètres de conservation.

Un compartiment avec le verrouillage d'objet S3 et la rétention par défaut configurés peut avoir téléchargé des objets 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 conservation lorsque la conservation par défaut est configurée. Les objets existants sans paramètres de conservation d'objet ne sont pas affectés.

Modes de rétention

La fonction de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de conservation Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
 - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
 - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date** : Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.



Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, reportez-vous à ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#).

Paramètre de rétention par défaut pour les compartiments

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent spécifier les paramètres par défaut suivants pour le compartiment :

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Reportez-vous à ["Créer un compartiment S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage d'objet S3"](#).

Comparaison du verrouillage d'objet S3 à la conformité existante

Le verrouillage d'objet S3 remplace la fonctionnalité de conformité disponible dans les versions précédentes de StorageGRID. Comme la fonctionnalité de verrouillage d'objet S3 est conforme aux exigences d'Amazon S3, elle déléguera la fonctionnalité propriétaire StorageGRID Compliance, qui est maintenant appelée « conformité héritée ».



Le paramètre de conformité global est obsolète. Si vous avez activé ce paramètre dans une version précédente de StorageGRID, le paramètre de verrouillage des objets S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, consultez ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#).

Si vous avez utilisé la fonctionnalité de conformité héritée dans une version précédente de StorageGRID, reportez-vous au tableau suivant pour savoir comment la comparer à la fonctionnalité de verrouillage d'objet S3 dans StorageGRID.

	Verrouillage d'objet S3	Conformité (existant)
Comment cette fonctionnalité est-elle activée dans le monde entier ?	Depuis le Gestionnaire de grille, sélectionnez Configuration > Système > Verrouillage d'objet S3 .	N'est plus pris en charge.
Comment la fonctionnalité est-elle activée pour un compartiment ?	Les utilisateurs doivent activer le verrouillage objet S3 lors de la création d'un compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3.	N'est plus pris en charge.
Le contrôle de version des compartiments est-il pris en	Oui. Le contrôle de version des compartiments est requis et activé automatiquement lorsque le verrouillage des objets S3 est activé pour le compartiment.	Non
Comment la conservation d'objets est-elle définie ?	Les utilisateurs peuvent définir une date de conservation jusqu'à pour chaque version d'objet ou définir une période de conservation par défaut pour chaque compartiment.	Les utilisateurs doivent définir une période de conservation pour l'intégralité du compartiment. La période de conservation s'applique à tous les objets du compartiment.
La période de conservation peut-elle être modifiée ?	• En mode conformité, la date de conservation jusqu'à la date d'un objet peut être augmentée, mais jamais réduite. • En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent diminuer, voire supprimer les paramètres de conservation d'un objet.	La période de rétention d'un godet peut être augmentée, mais jamais réduite.
Où est contrôlé la suspension légale ?	Les utilisateurs peuvent placer une conservation légale ou lever une conservation légale pour toute version d'objet dans le compartiment.	Une retenue légale est placée sur le godet et affecte tous les objets du godet.

	Verrouillage d'objet S3	Conformité (existant)
Quand les objets peuvent-ils être supprimés ?	- En mode de conformité, une version d'objet peut être supprimée une fois la date de conservation jusqu'à atteinte, en supposant que l'objet n'est pas en attente légale. - En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent supprimer un objet avant que sa date de conservation jusqu'à soit atteinte, en supposant que l'objet ne soit pas en attente légale.	Un objet peut être supprimé après l'expiration de la période de conservation, en supposant que le compartiment n'est pas en conservation légale. Les objets peuvent être supprimés automatiquement ou manuellement.
La configuration du cycle de vie des compartiments est-elle prise en	Oui	Non

Workflow de verrouillage d'objet S3 dans StorageGRID

En tant qu'administrateur du grid, vous devez coordonner étroitement avec les utilisateurs des locataires pour assurer la protection des objets conformément aux exigences de conservation.



L'application des paramètres de locataire sur l'ensemble du grid 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 du grid et aux utilisateurs de locataires contiennent des tâches de haut niveau relatives à l'utilisation de la fonction S3 Object Lock.

Administrateur du grid

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID.
- Autoriser les utilisateurs à activer le verrouillage d'objets S3 pour les compartiments existants.
- Assurez-vous que les politiques de gestion du cycle de vie des informations (ILM) sont *conformes*; c'est-à-dire ["Exigences des compartiments avec le verrouillage objet S3 activé"](#)-dire qu'elles respectent le .
- Si nécessaire, autorisez un locataire à utiliser le mode de conservation Compliance. Sinon, seul le mode gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Considérations relatives aux compartiments et aux objets avec le verrouillage d'objet S3
- Au besoin, contactez un administrateur de grille pour activer l'un des paramètres suivants :
 - Verrouillage d'objet global S3
 - Autoriser l'activation du verrouillage d'objets S3 pour les compartiments existants

- Créez des compartiments avec le verrouillage d'objet S3 activé.
- Activez le verrouillage des objets S3 sur les compartiments existants.
- Vous pouvez également configurer les paramètres de conservation par défaut d'un compartiment :
 - Mode de conservation par défaut : gouvernance ou conformité, si l'administrateur du grid l'autorise.
 - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application client S3 pour ajouter des objets et définir éventuellement la conservation propre à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si l'administrateur du grid l'autorise.
 - Conserver la date de fin : doit être inférieur ou égal à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Informations associées

Apprenez-en plus sur ["Exigences de verrouillage d'objet S3"](#)

Exigences de S3 Object Lock dans StorageGRID

Vous devez connaître les exigences relatives à l'activation du paramètre global de verrouillage d'objet S3, les exigences de création de règles ILM et de règles ILM conformes, et les restrictions StorageGRID placées sur des compartiments et des objets qui utilisent le verrouillage d'objet S3.

Conditions requises pour l'utilisation du paramètre global de verrouillage d'objet S3

- Vous devez activer le paramètre global de verrouillage d'objet S3 à l'aide de Grid Manager ou de l'API Grid Management avant qu'un locataire S3 puisse créer un compartiment avec le verrouillage d'objet S3 activé.
- L'activation du paramètre global de verrouillage d'objet S3 permet à tous les comptes de locataires S3 de créer des compartiments avec le verrouillage d'objet S3 activé.
- Une fois que vous avez activé le paramètre global S3 Object Lock, vous ne pouvez pas le désactiver.
- Vous ne pouvez pas activer le verrouillage d'objet S3 global à moins que la règle par défaut de toutes les règles ILM actives ne soit *conforme* (c'est-à-dire que la règle par défaut doit respecter les exigences des compartiments avec le verrouillage d'objet S3 activé).
- Lorsque le paramètre global S3 Object Lock est activé, vous ne pouvez pas créer de nouvelle règle ILM ou activer une règle ILM existante, sauf si la règle par défaut de la règle est conforme. Une fois le paramètre S3 Object Lock global activé, les pages de règles ILM et de règles ILM indiquent les règles ILM compatibles.

Conditions requises pour permettre l'activation du verrouillage d'objets S3 sur les compartiments existants

Lorsque le verrouillage global des objets S3 est activé, vous pouvez, si vous le souhaitez, autoriser tous les comptes locataires S3 ou utilisateurs S3 disposant des autorisations nécessaires à activer le verrouillage des objets S3 sur les compartiments existants. Lorsqu'un compte locataire S3 ou un utilisateur S3 active le verrouillage des objets S3 sur un compartiment existant, cela peut entraîner une migration des données d'un pool de stockage cloud vers StorageGRID, selon vos règles ILM.



Vous ne pouvez pas arrêter la migration des données non intentionnelle après son démarrage.

Exigences relatives aux règles ILM conformes

Si vous souhaitez activer le paramètre S3 Object Lock global, vous devez vous assurer que la règle par défaut de toutes les stratégies ILM actives est conforme. Une règle conforme répond aux exigences des deux compartiments avec le verrouillage de l'objet S3 activé et les compartiments existants pour lesquels la conformité de l'ancienne génération est activée :

- Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
- Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
- Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
- 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 « toujours ».

Exigences des règles ILM

Lorsque le paramètre global S3 Object Lock est activé, les règles ILM actives et inactives peuvent inclure des règles conformes et non conformes.

- La règle par défaut d'une politique ILM active ou inactive doit être conforme.
- Les règles non conformes s'appliquent uniquement aux objets des compartiments qui ne disposent pas du verrouillage d'objet S3 ou qui ne disposent pas de la fonctionnalité conformité héritée.
- Les règles conformes peuvent s'appliquer aux objets dans n'importe quel compartiment. Il n'est pas nécessaire d'activer le verrouillage objet S3 ou la conformité héritée.

"Exemple de règle ILM conforme pour le verrouillage objet S3"

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors du téléchargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client S3 ou de l'API REST S3.

- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. Entrée d'objet

Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

- Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment par défaut sont ignorés.
- Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
- Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par le verrouillage objet S3.

Si les paramètres de conservation sont appliqués, l'objet et les métadonnées S3 définies par l'utilisateur sont protégés.

2. Conservation et suppression d'objets

StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité dans les politiques ILM actives. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

- Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Informations associées

- ["Créer un compartiment S3"](#)
- ["Mettre à jour la conservation par défaut du verrouillage d'objet S3"](#)
- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3"](#)

Activer le verrouillage d'objets S3 dans StorageGRID

Si un compte de locataire S3 doit respecter les exigences réglementaires lors de la sauvegarde des données d'objet, vous devez activer le verrouillage objet S3 pour l'intégralité de votre système StorageGRID. L'activation du paramètre de verrouillage d'objet S3 global permet aux locataires S3 de créer et de gérer des compartiments et des objets avec le verrouillage d'objet S3.

Avant de commencer

- Vous avez le ["Autorisation d'accès racine"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez examiné le workflow de verrouillage d'objet S3 et vous en avez pris connaissance.
- Vous avez confirmé que la règle par défaut de la stratégie ILM active est conforme. Consultez ["Créez une règle ILM par défaut"](#) pour plus de détails.

Description de la tâche

Un administrateur de grid doit activer le paramètre global de verrouillage d'objet S3 pour permettre aux utilisateurs locataires de créer de nouveaux compartiments pour lesquels le verrouillage d'objet S3 est activé. Une fois ce paramètre activé, il ne peut pas être désactivé.

Après avoir activé le verrouillage d'objet S3, un administrateur de grille peut également autoriser les utilisateurs du locataire à activer le verrouillage d'objet S3 sur un compartiment existant. Après qu'un administrateur de grille a activé ce paramètre, il peut le désactiver. Pour plus d'informations, consultez ["Exigences de verrouillage d'objet S3"](#).

Vérifiez les paramètres de conformité des locataires existants après avoir activé le paramètre global S3 Object Lock. 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 dans une version précédente de StorageGRID, le paramètre de verrouillage des objets S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, consultez ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération 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** pour activer le verrouillage d'objet S3 pour l'ensemble de votre système StorageGRID.
3. Vous pouvez également sélectionner **Autoriser l'activation du verrouillage d'objets S3 sur les compartiments existants**.



L'activation du verrouillage d'objet S3 sur un compartiment existant peut entraîner une migration des données d'un pool de stockage cloud vers StorageGRID, selon vos règles ILM. Vous ne pouvez pas arrêter cette migration une fois qu'elle a commencé. Pour plus d'informations, consultez ["Exigences de verrouillage d'objet S3"](#).

4. Sélectionnez **appliquer**.

Une boîte de dialogue de confirmation s'affiche et vous rappelle que vous ne pouvez pas désactiver le verrouillage d'objet S3 après son activation.

5. Si vous êtes sûr de vouloir activer définitivement le verrouillage d'objet S3 pour l'ensemble du système, sélectionnez **OK**.

Lorsque vous sélectionnez **OK**:

- Si la règle par défaut de la règle ILM active est conforme, le verrouillage d'objet S3 est désormais activé pour l'ensemble de la grille et ne peut pas être désactivé.
- Si la règle par défaut n'est pas conforme, une erreur s'affiche. Vous devez créer et activer une nouvelle stratégie ILM qui inclut une règle conforme comme règle par défaut. Sélectionnez **OK**. Ensuite, créez une nouvelle stratégie, simulez-la et activez-la. Consultez "[Création de la règle ILM](#)" pour obtenir des instructions.

Résolvez les erreurs de cohérence lors de la mise à jour de S3 Object Lock ou des paramètres de conformité hérités dans StorageGRID

Si un site de data Center ou plusieurs nœuds de stockage sur un site deviennent indisponibles, les locataires S3 peuvent avoir à appliquer des modifications à la configuration de verrouillage d'objet S3 ou de conformité héritée.

Les locataires qui utilisent des compartiments avec le verrouillage d'objet S3 (ou la conformité héritée) peuvent modifier certains paramètres. Par exemple, un utilisateur locataire qui utilise le verrouillage objet S3 peut avoir à mettre une version d'objet en attente légale.

Lorsqu'un locataire met à jour les paramètres d'un compartiment S3 ou d'une version d'objet, StorageGRID tente immédiatement de mettre à jour les métadonnées du compartiment ou de l'objet dans la grille. Si le système ne peut pas mettre à jour les métadonnées car un site de data Center ou plusieurs nœuds de stockage ne sont pas disponibles, une erreur s'affiche :

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Pour résoudre cette erreur, procédez comme suit :

1. Essayez de rendre tous les nœuds ou sites de stockage disponibles à nouveau dès que possible.
2. Si vous ne pouvez pas rendre suffisamment de nœuds de stockage disponibles sur chaque site, contactez le support technique qui peut vous aider à restaurer les nœuds et veiller à ce que les modifications soient appliquées de manière cohérente dans l'ensemble de la grille.
3. Une fois le problème sous-jacent résolu, rappelez à l'utilisateur locataire de réessayer de modifier sa configuration.

Informations associées

- "[Utilisez un compte de locataire](#)"
- "[UTILISEZ L'API REST S3](#)"
- "[Récupérer et entretenir](#)"

Exemples de règles et de règles ILM

Règles ILM et politique pour la protection et la conservation de base des objets dans StorageGRID

Vous pouvez utiliser les exemples de règles et de règle suivants comme point de départ pour définir une règle ILM afin de répondre à vos exigences de protection et de

conservation des objets.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d’activer une nouvelle stratégie, simulez-la pour confirmer qu’elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1, exemple 1 : copie des données d’objet vers deux sites

Cet exemple de règle ILM copie les données d’objet dans des pools de stockage de deux sites.

Définition de règle	Exemple de valeur
Pools de stockage sur un site	Deux pools de stockage, chacun contenant des sites différents, nommés site 1 et site 2.
Nom de la règle	Deux copies deux sites
Heure de référence	Temps d’ingestion
Placements	Du jour 0 à l’infini, conservez une copie répliquée sur le site 1 et une copie répliquée sur le site 2.

La section analyse des règles du diagramme de rétention indique :

- La protection contre la perte de site StorageGRID s’appliquera pendant toute la durée de cette règle.
- Les objets traités par cette règle ne seront pas supprimés par ILM.

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, exemple 1 : profil de code d'effacement avec mise en correspondance des compartiments

Cet exemple de règle ILM utilise un profil de code d'effacement et un compartiment S3 pour déterminer l'emplacement et la durée de stockage de l'objet.

Définition de règle	Exemple de valeur
Pool de stockage avec plusieurs sites	- Un pool de stockage sur trois sites (sites 1, 2, 3) - Utilisez le schéma de code d'effacement 6+3
Nom de la règle	Dossiers financiers du compartiment S3
Heure de référence	Temps d'ingestion
Placements	Pour les objets du compartiment S3 nommés finance-records, créez une copie avec code d'effacement dans le pool spécifié par le profil de code d'effacement. Conserver cette copie pour toujours.

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

Forever

Règle ILM, par exemple 1

Dans la pratique, la plupart des règles ILM sont simples, même si le système StorageGRID vous permet de concevoir des règles ILM complexes et sophistiquées.

Une règle ILM standard pour un grid multisite peut inclure des règles ILM, telles que :

- Lors de l'ingestion, stockez tous les objets appartenant au compartiment S3 nommé `finance-records` dans un pool de stockage contenant trois sites. Utilisez le code d'effacement 6+3.
- Si un objet ne correspond pas à la première règle ILM, utilisez la règle ILM par défaut de la règle, deux copies de data centers, pour stocker une copie de cet objet sur le site 1 et une copie sur le site 2.

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 associées

- ["Règles ILM"](#)
- ["Création de règles ILM"](#)

Règles ILM et politique pour le filtrage de la taille des objets EC dans StorageGRID

Des exemples de règles et de règles ci-dessous vous permettent de définir une règle ILM qui s'applique par taille d'objet afin de répondre aux exigences EC recommandées.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1, par exemple 2 : utilise ce pour les objets de plus de 1 Mo

Cet exemple de règle ILM code des objets dont le nombre est supérieur à 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	Objets EC uniquement > 1 Mo
Heure de référence	Temps d'ingestion
Filtre avancé pour la taille de l'objet	Taille de l'objet supérieure à 1 Mo
Placements	Créez une copie avec code d'effacement 2+1 sur trois sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ×

Object size ▼

greater than ▼

1 ↕

MB ▼ ×

Règle ILM 2, par exemple 2 : deux copies répliquées

Cet exemple de règle ILM crée deux copies répliquées, sans filtrer par taille d'objet. Cette règle est la règle par défaut de la règle. Étant donné que la première règle filtre tous les objets de plus de 1 Mo, cette règle s'applique uniquement aux objets de 1 Mo ou plus.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Heure de référence	Temps d'ingestion

Définition de règle	Exemple de valeur
Filtre avancé pour la taille de l'objet	Aucune
Placements	Du jour 0 à l'infini, conservez une copie répliquée sur le site 1 et une copie répliquée sur le site 2.

Règle ILM par exemple 2 : utilisez l'effacement pour des objets supérieurs à 1 Mo

Cet exemple de règle ILM inclut deux règles ILM :

- La première règle code tous les objets supérieurs à 1 Mo.
- La seconde règle ILM (par défaut) crée deux copies répliquées. Étant donné que les objets de plus de 1 Mo ont été filtrés par la règle 1, la règle 2 ne s'applique qu'aux objets de 1 Mo ou moins.

Règles et politique ILM pour la protection des fichiers image dans StorageGRID

Vous pouvez utiliser les règles et règles suivantes pour vous assurer que les images de plus de 1 Mo sont codées avec effacement et que deux copies sont réalisées avec des images de plus petite taille.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1 par exemple 3 : utilisez EC pour les fichiers image de plus de 1 Mo

Cet exemple de règle ILM utilise un filtrage avancé pour coder d'effacement de tous les fichiers image de plus de 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	Fichiers image EC > 1 Mo
Heure de référence	Temps d'ingestion
Filtre avancé pour la taille de l'objet	Taille de l'objet supérieure à 1 Mo
Filtres avancés pour la clé	• Se termine par .jpg • Se termine par .png
Placements	Créez une copie avec code d'effacement 2+1 sur trois sites

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

X

and

Key

ends with

.jpg

X

or
Filter group 2
Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

X

and

Key

ends with

.png

X

Étant donné que cette règle est configurée comme la première règle de la règle, l'instruction de placement de code d'effacement s'applique uniquement aux fichiers .jpg et .png de plus de 1 Mo.

Règle ILM 2, par exemple 3 : création de 2 copies répliquées pour tous les fichiers d'images restants

Cet exemple de règle ILM utilise un filtrage avancé pour spécifier la réplcation de fichiers d'images plus petits. Comme la première règle de la stratégie a déjà mis en correspondance des fichiers d'image de plus de 1 Mo, cette règle s'applique aux fichiers d'image de 1 Mo ou moins.

Définition de règle	Exemple de valeur
Nom de la règle	2 copies pour les fichiers image
Heure de référence	Temps d'ingestion
Filtres avancés pour la clé	- Se termine par .jpg - Se termine par .png
Placements	Créez 2 copies répliquées dans deux pools de stockage

Règle ILM, par exemple 3 : meilleure protection des fichiers image

Cet exemple de règle ILM comprend trois règles :

- La première règle code tous les fichiers image de plus de 1 Mo.
- La deuxième règle crée deux copies de tous les fichiers d'image restants (c'est-à-dire les images de 1 Mo ou plus).
- La règle par défaut s'applique à tous les objets restants (c'est-à-dire tous les fichiers non images).

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	—

Règles et politiques ILM pour les versions non actuelles des objets S3 dans StorageGRID

Si la gestion des versions est activée dans un compartiment S3, vous pouvez gérer les versions d'objets non actuelles en incluant des règles dans votre règle ILM qui utilisent l'heure non courante comme heure de référence.



Si vous spécifiez une durée de conservation limitée pour les objets, ces objets seront supprimés définitivement après la période de temps atteinte. Assurez-vous de bien comprendre la durée pendant laquelle les objets seront conservés.

Comme le montre cet exemple, vous pouvez contrôler la quantité de stockage utilisée par les objets avec version à l'aide d'instructions de placement différentes pour les versions d'objets non actuelles.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.



Pour effectuer une simulation de règle ILM sur une version non actuelle d'un objet, vous devez connaître l'UUID ou CBID de la version de l'objet. Pour rechercher l'UUID et le CBID, utilisez ["recherche de métadonnées d'objet"](#) tant que l'objet est toujours à jour.

Règle ILM 1, par exemple 4 : trois copies économisées sur 10 ans

Cet exemple de règle ILM stocke une copie de chaque objet sur trois sites pendant 10 ans.

Cette règle s'applique à tous les objets, qu'ils soient versionnés ou non.

Définition de règle	Exemple de valeur
Pools de stockage	Trois pools de stockage, chacun étant constitué de data centers différents : site 1, site 2 et site 3.
Nom de la règle	Trois copies dix ans
Heure de référence	Temps d'ingestion

Définition de règle	Exemple de valeur
Placements	Au jour 0, conservez trois copies répliquées pendant 10 ans (3,652 jours), une dans le site 1, une dans le site 2 et une dans le site 3. Au bout de 10 ans, supprimez toutes les copies de l'objet.

Règle ILM 2, par exemple 4 : enregistrez deux copies de versions non actuelles pendant 2 ans

Cet exemple de règle ILM stocke deux copies des versions non actuelles d'un objet avec version S3 pendant 2 ans.

La règle ILM 1 s'applique à toutes les versions de l'objet, c'est pourquoi vous devez créer une autre règle pour filtrer toutes les versions non actuelles.

Pour créer une règle qui utilise « Noncurrent Time » comme heure de référence, sélectionnez **Oui** pour la question, « appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec multiversion activée) ? » À l'étape 1 (entrer les détails) de l'assistant de création de règles ILM. Lorsque vous sélectionnez **Oui**, *Noncurrent Time* est automatiquement sélectionné pour l'heure de référence et vous ne pouvez pas sélectionner une autre heure de référence.

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 règle	Exemple de valeur
Pools de stockage	Deux pools de stockage, situés chacun au niveau de data centers différents : site 1 et site 2.
Nom de la règle	Versions non actuelles : deux copies deux ans
Heure de référence	Heure non actuelle Sélection automatique lorsque vous sélectionnez Oui pour la question « appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée) ? » Dans l'assistant de création d'une règle ILM.
Placements	Le jour 0 par rapport à l'heure non courante (c'est-à-dire, à partir du jour où la version de l'objet devient la version non actuelle), conserver deux copies répliquées des versions de l'objet non actuel pendant 2 ans (730 jours), une dans le site 1 et une dans le site 2. À la fin de 2 ans, supprimer les versions non actuelles.

Règle ILM, par exemple 4 : objets avec version S3

Si vous souhaitez gérer des versions plus anciennes d'un objet différemment de la version actuelle, les règles qui utilisent l'heure « Noncurrent Time » comme heure de référence doivent apparaître dans la politique ILM avant les règles qui s'appliquent à la version d'objet actuelle.

Une règle ILM pour les objets avec version S3 peut inclure des règles ILM :

- Conservez les versions plus anciennes (non actuelles) de chaque objet pendant 2 ans, à partir du jour où la version n'est plus à jour.



Les règles « temps non courant » doivent apparaître dans la stratégie avant les règles qui s'appliquent à la version d'objet actuelle. Sinon, les versions d'objet non actuelles ne seront jamais mises en correspondance avec la règle « Noncurrent Time ».

- Lors de l'ingestion, créez trois copies répliquées et stockez une copie sur chacun des trois sites. Conservez les copies de la version actuelle de l'objet pendant 10 ans.

Lorsque vous simulez l'exemple de stratégie, vous vous attendez à ce que les objets test soient évalués comme suit :

- Toutes les versions d'objet non courantes seront mises en correspondance par la première règle. Si une version d'objet non actuelle a plus de 2 ans, elle est supprimée définitivement par ILM (toutes les copies de la version non actuelle sont supprimées de la grille).
- La version actuelle de l'objet sera comparée à la seconde règle. Lorsque la version actuelle de l'objet est 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 est mise en correspondance avec la première règle. Par conséquent, la copie sur le site 3 est purgée et les deux copies sur le site 1 et le site 2 sont conservées pendant 2 ans supplémentaires.

Informations associées

Règles et politiques ILM pour un comportement d'ingestion strict dans StorageGRID

Vous pouvez utiliser un filtre d'emplacement et un comportement d'ingestion strict dans une règle pour empêcher la sauvegarde des objets dans un emplacement de data Center spécifique.

Dans cet exemple, un locataire basé à Paris ne veut pas stocker certains objets en dehors de l'UE en raison de préoccupations réglementaires. Les autres objets, et notamment tous les objets des autres comptes locataires, peuvent être stockés dans le data Center de Paris ou dans le data Center des États-Unis.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Informations associées

- ["Options d'ingestion"](#)
- ["Créer une règle ILM : sélectionnez le comportement d'ingestion"](#)

La règle ILM 1, par exemple 5 : une ingestion stricte pour la garantie du data Center Paris

Cet exemple de règle ILM utilise un comportement d'ingestion strict afin de garantir que les objets enregistrés par un locataire Paris dans des compartiments S3 avec la région UE-West-3 (Paris) ne sont jamais stockés dans le data Center des États-Unis.

Cette règle s'applique aux objets appartenant au locataire Paris et dont la région du compartiment S3 est définie sur eu-West-3 (Paris).

Définition de règle	Exemple de valeur
Compte locataire	Locataire Paris
Filtre avancé	Contrainte de localisation égale à eu-West-3
Pools de stockage	Site 1 (Paris)
Nom de la règle	Ingestion stricte pour le data Center de Paris
Heure de référence	Temps d'ingestion
Placements	Au jour 0, conservation de deux copies répliquées pour toujours dans le site 1 (Paris)
Comportement d'ingestion	Stricte. Utilisez toujours les placements de cette règle lors de l'entrée. L'ingestion échoue s'il est impossible de stocker deux copies de l'objet dans le data Center de Paris.

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.



La règle ILM 2, par exemple 5, « ingestion équilibrée » pour d'autres objets

Cet exemple de règle ILM utilise le comportement d'ingestion équilibré pour offrir une efficacité ILM optimale pour tous les objets qui ne sont pas mis en correspondance avec la première règle. Deux copies de tous les objets correspondant à cette règle seront stockées : une dans le data Center des États-Unis et une dans le data Center de Paris. Si la règle ne peut pas être satisfaite immédiatement, les copies provisoires sont stockées à n'importe quel emplacement disponible.

Cette règle s'applique aux objets appartenant à n'importe quel locataire et à n'importe quelle région.

Définition de règle	Exemple de valeur
Compte locataire	Ignorer
Filtre avancé	Non spécifié
Pools de stockage	Site 1 (Paris) et site 2 (US)
Nom de la règle	2 copies 2 data centers
Heure de référence	Temps d'ingestion

Définition de règle	Exemple de valeur
Placements	Au premier jour, conservez deux copies répliquées à jamais dans deux data centers
Comportement d'ingestion	Équilibré. Si possible, les objets qui correspondent à cette règle sont placés conformément aux instructions de positionnement de la règle. Dans le cas contraire, des copies provisoires sont effectuées à tout emplacement disponible.

Règle ILM, par exemple 5 : combinaison de comportements d'ingestion

L'exemple de règle ILM comprend deux règles ayant des comportements d'entrée différents.

Deux règles ILM sont appliquées à deux comportements d'ingestion, notamment :

- Stockez des objets qui appartiennent au locataire Paris et qui disposent de la région du compartiment S3 définie sur eu-West-3 (Paris) uniquement dans le data Center de Paris. Echec de l'ingestion si le centre de données Paris n'est pas disponible.
- Stockez tous les autres objets (y compris ceux qui appartiennent à un locataire Paris mais qui disposent d'une région de compartiment différente) dans le data Center américain et dans le data Center de Paris. Faites des copies intermédiaires à n'importe quel emplacement disponible si l'instruction de placement ne peut pas être satisfaite.

Lorsque vous simulez l'exemple de stratégie, vous vous attendez à ce que les objets test soient évalués comme suit :

- Tous les objets qui appartiennent au locataire Paris et qui disposent de la région du compartiment S3 définie sur eu-West-3 sont mis en correspondance par la première règle et stockés dans le data Center de Paris. La première règle utilise une ingestion stricte. Ces objets ne sont donc jamais stockés dans le data Center des États-Unis. Si les nœuds de stockage du data Center de Paris ne sont pas disponibles, l'ingestion échoue.
- Tous les autres objets sont comparés à la seconde règle, y compris les objets appartenant au locataire Paris et dont la région de compartiment S3 n'est pas définie sur eu-West-3. Une copie de chaque objet est enregistrée dans chaque data Center. Cependant, la seconde règle utilise une ingestion équilibrée, si un data Center n'est plus disponible, deux copies intermédiaires sont enregistrées à tout emplacement disponible.

Comment la modification d'une politique ILM affecte les performances de StorageGRID

Si vous devez modifier la protection de vos données ou ajouter de nouveaux sites, vous pouvez créer et activer une nouvelle règle ILM.

Avant de modifier une règle, vous devez savoir comment les modifications apportées aux règles ILM peuvent affecter temporairement les performances globales d'un système StorageGRID.

Dans cet exemple, un nouveau site StorageGRID a été ajouté dans une extension et une nouvelle règle ILM active doit être implémentée pour stocker les données sur le nouveau site. Pour mettre en œuvre une nouvelle politique active, d'abord **"créer une règle"**. Ensuite, vous devez, **"simuler"** puis **"activer"** la nouvelle police.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Impact de la modification d'une règle ILM sur les performances

Lorsque vous activez une nouvelle règle ILM, les performances de votre système StorageGRID peuvent être temporairement affectées, en particulier si les instructions de placement dans la nouvelle règle requièrent le déplacement d'un grand nombre d'objets existants vers de nouveaux emplacements.

Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Pour vous assurer qu'une nouvelle règle ILM n'affecte pas le placement des objets répliqués et soumis au code d'effacement, vous pouvez "[Créez une règle ILM avec un filtre de temps d'ingestion](#)". Par exemple, **heure d'ingestion est on ou after <date and time>**, de sorte que la nouvelle règle s'applique uniquement aux objets ingérés à la date et à l'heure spécifiées ou après.

Les types de modifications de règles ILM susceptibles d'affecter temporairement les performances de StorageGRID sont les suivants :

- Appliquer un profil de code d'effacement différent aux objets existants avec code d'effacement.



StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

- Modification du type de copies requis pour les objets existants (par exemple, conversion d'un grand pourcentage d'objets répliqués en objets avec code d'effacement).
- Déplacement des copies d'objets existants vers un emplacement totalement différent (par exemple, déplacement d'un grand nombre d'objets vers ou depuis un pool de stockage cloud, vers ou depuis un site distant).

Règle ILM active, par exemple 6 : protection des données sur deux sites

Dans cet exemple, la politique ILM active a été initialement conçue pour un système StorageGRID à deux sites et utilise deux règles ILM.

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 code d'effacement 2+1 sur un seul site, tandis que les objets de tous les autres locataires sont protégés sur deux sites à l'aide de la réplication à 2 copies.

Règle 1 : code d'effacement sur un site pour le locataire A

Définition de règle	Exemple de valeur
Nom de la règle	Code d'effacement sur un site pour le locataire A
Compte de locataire	Locataire A
Pool de stockage	Site 1
Placements	Code d'effacement 2+1 sur le site 1, du jour 0 à l'infini

Règle 2 : réplication sur deux sites pour d'autres locataires

Définition de règle	Exemple de valeur
Nom de la règle	Réplication sur deux sites pour d'autres locataires
Compte de locataire	Ignorer
Pools de stockage	Site 1 et site 2
Placements	Deux copies répliquées du jour 0 au jour toujours : une copie sur le site 1 et une copie sur le site 2.

Règle ILM, exemple 6 : protection des données sur trois sites

Dans cet exemple, la politique ILM est remplacée par une nouvelle règle pour un système StorageGRID à trois sites.

Après avoir effectué une extension pour ajouter le nouveau site, l'administrateur de la grille a créé deux nouveaux pools de stockage : un pool de stockage pour le site 3 et un pool de stockage contenant les trois sites (différent du pool de stockage par défaut de tous les nœuds de stockage). L'administrateur a ensuite créé deux nouvelles règles ILM et une nouvelle politique ILM, conçue pour protéger les données des trois sites.

Lors de l'activation de cette nouvelle politique ILM, les objets appartenant au locataire A seront protégés par un code d'effacement 2+1 sur trois sites, tandis que les objets appartenant à d'autres locataires (et les objets de plus petite taille appartenant au locataire A) sont protégés sur trois sites à l'aide de la réplication à 3 copies.

Règle 1 : code d'effacement à trois sites pour le locataire A

Définition de règle	Exemple de valeur
Nom de la règle	Code d'effacement à trois sites pour le locataire A
Compte de locataire	Locataire A
Pool de stockage	Tous les sites 3 (y compris le site 1, le site 2 et le site 3)
Placements	Code d'effacement 2+1 sur les 3 sites, du jour 0 à l'infini

Règle 2 : réplication sur trois sites pour d'autres locataires

Définition de règle	Exemple de valeur
Nom de la règle	Réplication sur trois sites pour les autres locataires
Compte de locataire	Ignorer
Pools de stockage	Site 1, site 2 et site 3
Placements	Trois copies répliquées du jour 0 au jour toujours : une copie sur le site 1, une copie sur le site 2 et une copie sur le site 3.

Activation de la stratégie ILM, par exemple 6

Lorsque vous activez une nouvelle règle ILM, les objets existants peuvent être déplacés vers de nouveaux emplacements ou de nouvelles copies d'objets peuvent être créées pour des objets existants, en fonction des instructions de placement dans les règles nouvelles ou mises à jour.



Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Que se passe-t-il en cas de modification des instructions de code d'effacement

Dans cet exemple de règle ILM active, les objets appartenant au locataire A sont protégés par un code d'effacement 2+1 sur le site 1. Dans la nouvelle politique ILM, les objets appartenant au locataire A seront protégés par un code d'effacement 2+1 sur les sites 1, 2 et 3.

Lorsque la nouvelle règle ILM est activée, les opérations ILM suivantes se produisent :

- Les nouveaux objets ingérés par le locataire A sont divisés en deux fragments de données et un fragment de parité est ajouté. Ensuite, chacun des trois fragments est stocké sur un site différent.
- Les objets existants appartenant au locataire A sont réévalués au cours du processus d'analyse ILM en cours. Les instructions de placement ILM utilisent un nouveau profil de code d'effacement, c'est pourquoi de nouveaux fragments avec code d'effacement sont créés et distribués sur les trois sites.



Les fragments 2+1 existants au site 1 ne sont pas réutilisés. StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

Ce qui se passe lorsque les instructions de réplication changent

Dans cet exemple de règle ILM active, les objets appartenant à d'autres locataires sont protégés par deux copies répliquées dans les pools de stockage des sites 1 et 2. Dans la nouvelle règle ILM, les objets appartenant à d'autres locataires seront protégés par trois copies répliquées dans les pools de stockage des sites 1, 2 et 3.

Lorsque la nouvelle règle ILM est activée, les opérations ILM suivantes se produisent :

- Lorsqu'un locataire autre que le locataire A ingère un nouvel objet, StorageGRID crée trois copies et enregistre une copie sur chaque site.
- Les objets existants appartenant à ces autres locataires sont réévalués en cours d'analyse ILM. Étant donné que les copies d'objet existantes sur le site 1 et le site 2 continuent à satisfaire les exigences de réplication de la nouvelle règle ILM, StorageGRID ne doit créer qu'une seule copie de l'objet pour le site 3.

Impact sur les performances de l'activation de cette stratégie

Lorsque la politique ILM de cet exemple est activée, les performances globales de ce système StorageGRID seront temporairement affectées. Des niveaux de ressources de grid supérieurs à la normale seront nécessaires pour créer de nouveaux fragments avec code d'effacement pour les objets existants du locataire A et pour les nouvelles copies répliquées sur le site 3 pour les objets existants des autres locataires.

Suite à une modification de la règle ILM, les demandes de lecture et d'écriture des clients peuvent présenter temporairement des latences supérieures à la normale. Une fois que les instructions de placement sont entièrement mises en œuvre sur la grille, les latences reprennent aux niveaux normaux.

Pour éviter les problèmes de ressources lors de l'activation d'une nouvelle stratégie ILM, vous pouvez utiliser

le filtre avancé heure d'ingestion dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion sur une valeur supérieure ou égale à la durée approximative de l'entrée en vigueur de la nouvelle règle pour vous assurer que les objets existants ne sont pas déplacés inutilement.



Contactez le support technique si vous avez besoin de ralentir ou d'augmenter le taux de traitement des objets après une modification de la règle ILM.

Stratégie ILM conforme pour S3 Object Lock dans StorageGRID

Vous pouvez utiliser le compartiment S3, les règles ILM et la règle ILM dans cet exemple à partir d'un point de départ lors de la définition d'une règle ILM afin de répondre aux exigences de protection et de conservation des objets dans des compartiments où le verrouillage d'objet S3 est activé.



Si vous avez utilisé la fonctionnalité de conformité héritée dans les versions précédentes de StorageGRID, vous pouvez également utiliser cet exemple pour gérer les compartiments existants pour lesquels la fonctionnalité de conformité héritée est activée.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Informations associées

- ["Gestion des objets avec le verrouillage d'objets S3"](#)
- ["Créer une règle ILM"](#)

Exemple de compartiment et d'objets pour le verrouillage d'objet S3

Dans cet exemple, un compte de locataire S3 nommé Bank of ABC a utilisé le gestionnaire de locataires pour créer un compartiment avec le verrouillage objet S3 activé pour stocker les enregistrements bancaires stratégiques.

Définition du compartiment	Exemple de valeur
Nom du compte du locataire	Banque d'ABC
Nom du compartiment	les registres bancaires
Région du godet	us-east-1 (par défaut)

Chaque objet et version d'objet ajoutés au compartiment des enregistrements de banque utilise les valeurs suivantes pour les `retain-until-date` paramètres et `legal hold`.

Paramètre pour chaque objet	Exemple de valeur
<code>retain-until-date</code>	« 2030-12-30T23:59:59Z » (30 décembre 2030) Chaque version d'objet a son propre <code>retain-until-date</code> paramètre. Ce réglage peut être augmenté, mais pas diminué.
<code>legal hold</code>	« OFF » (DÉSACTIVÉ) (non en vigueur) Une mise en garde légale peut être placée ou levée sur n'importe quelle version d'objet à tout moment pendant la période de conservation. Si un objet est en attente légale, il ne peut pas être supprimé même si <code>retain-until-date</code> a été atteint.

Règle ILM 1 pour S3 Object Lock exemple : profil de code d'effacement avec mise en correspondance des compartiments

Cet exemple de règle ILM s'applique uniquement au compte de locataire S3 nommé Bank of ABC. Elle fait correspondre n'importe quel objet du `bank-records` compartiment, puis utilise le code d'effacement pour stocker l'objet sur les nœuds de stockage situés sur trois sites de data Center à l'aide d'un profil de code d'effacement 6+3. Cette règle satisfait aux exigences des compartiments avec S3 Object Lock activé : une copie est conservée sur les nœuds de stockage du jour 0 à l'infini, en utilisant l'heure d'ingestion comme heure de référence.

Définition de règle	Exemple de valeur
Nom de la règle	Règle de conformité : objets EC dans le compartiment des enregistrements bancaires - Banque d'ABC
Compte de locataire	Banque d'ABC
Nom du compartiment	<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 plus.

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	À partir du jour 0 magasin pour toujours
Profil de code d'effacement	• Créez une copie avec code d'effacement sur les nœuds de stockage de trois sites de data Center • Utilisez le schéma de code d'effacement 6+3

Règle ILM 2 pour exemple de verrouillage d'objet S3 : règle non compatible

Cet exemple de règle ILM stocke au départ deux copies d'objet répliquées sur les nœuds de stockage. Après un an, il stocke une copie sur un pool de stockage cloud pour toujours. Cette règle utilise un pool de stockage cloud. Elle n'est pas conforme et ne s'applique pas aux objets des compartiments où le verrouillage des objets S3 est activé.

Définition de règle	Exemple de valeur
Nom de la règle	Règle non conforme : utilisez le pool de stockage cloud
Comptes de locataires	Non spécifié
Nom du compartiment	Non spécifié, mais s'appliquera uniquement aux compartiments pour lesquels le verrouillage d'objet S3 (ou la fonction conformité héritée) n'est pas activé.
Filtre avancé	Non spécifié

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	• Le premier jour, conservez deux copies répliquées sur les nœuds de stockage dans le data Center 1 et dans le data Center 2 pendant 365 jours • Après 1 an, conservez une copie répliquée dans un pool de stockage cloud à jamais

Règle ILM 3 pour l'exemple de verrouillage d'objet S3 : règle par défaut

Cet exemple de règle ILM copie les données d'objet vers les pools de stockage dans deux data centers. Cette règle conforme est conçue pour être la règle par défaut dans la politique ILM. Elle n'inclut aucun filtre, n'utilise pas l'heure de référence non actuelle et répond aux exigences des compartiments avec le verrouillage objet S3 activé : deux copies d'objet sont conservées sur les nœuds de stockage du jour 0 à l'infini, et l'ingestion comme heure de référence.

Définition de règle	Exemple de valeur
Nom de la règle	Règle de conformité par défaut : deux copies de deux data centers
Compte locataire	Non spécifié
Nom du compartiment	Non spécifié
Filtre avancé	Non spécifié

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	Dès le premier jour, conservez deux copies répliquées : une sur des nœuds de stockage dans le data Center 1 et une sur des nœuds de stockage dans le data Center 2.

Exemple de règle ILM conforme pour l'exemple de verrouillage d'objet S3

Pour créer une règle ILM protégeant efficacement tous les objets de votre système, y compris ceux des compartiments avec le verrouillage objet S3 activé, vous devez sélectionner des règles ILM qui répondent aux besoins de stockage de tous les objets. Vous devez ensuite simuler et activer la règle.

Ajouter des règles à la règle

Dans cet exemple, la politique ILM inclut trois règles ILM, dans l'ordre suivant :

1. Règle conforme qui utilise le code d'effacement pour protéger les objets de plus de 1 Mo dans un compartiment spécifique avec le verrouillage objet S3 activé. Les objets sont stockés sur les nœuds de stockage du premier jour vers toujours.
2. Une règle non conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage pendant un an, puis déplace une copie d'objet vers un pool de stockage cloud à tout moment. Cette règle ne s'applique pas aux compartiments avec le verrouillage d'objet S3 activé car elle utilise un pool de stockage cloud.
3. La règle de conformité par défaut qui crée deux copies d'objets répliquées sur les nœuds de stockage du jour 0 à l'infini.

Simuler la règle

Après avoir ajouté des règles à votre stratégie, choisissez une règle de conformité par défaut et organisez les autres règles, vous devez simuler la stratégie en testant les objets à partir du compartiment avec S3 Object Lock activé et à partir d'autres compartiments. Par exemple, lorsque vous simulez l'exemple de règle, vous attendez à ce que les objets test soient évalués comme suit :

- La première règle correspond uniquement aux objets de test supérieurs à 1 Mo dans les banques d'enregistrements du compartiment pour le locataire Bank of ABC.
- La deuxième règle fait correspondre tous les objets de tous les compartiments non conformes pour tous les autres comptes de tenant.
- La règle par défaut correspond à ces objets :
 - Objets de 1 Mo ou plus petits dans les banques d'enregistrements du compartiment pour le locataire Banque d'ABC.
 - Objets dans tout autre compartiment pour lequel le verrouillage objet S3 est activé pour tous les autres comptes locataires.

Activer la règle

Si vous êtes pleinement satisfait de la nouvelle règle assurant la protection des données d'objet comme prévu, vous pouvez l'activer.

Comment le cycle de vie des compartiments S3 et la politique ILM interagissent dans StorageGRID

Selon la configuration du cycle de vie, les objets suivent les paramètres de conservation du cycle de vie du compartiment S3 ou une règle ILM.

Exemple de cycle de vie du compartiment qui est prioritaire sur la règle ILM

Politique ILM

- Règle basée sur une référence d'heure non courante : au jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence d'heure d'entrée (par défaut) : au jour 0, conserver X copies pendant 50 jours

Cycle de vie du godet

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Elle correspond au filtre de cycle de vie du compartiment du préfixe « docs/ ».
 - Au bout de 100 jours, un marqueur de suppression est créé et « docs/text » n'est plus à jour.
 - Au bout de 5 jours, 105 jours au total depuis l'entrée, « docs/text » est supprimé.
 - Après 95 jours, soit un total de 200 jours depuis l'entrée et de 100 jours depuis la création du marqueur de suppression, le marqueur de suppression périmé est supprimé.
- Un objet nommé « vidéo/film » est ingéré. Elle ne correspond pas au filtre et utilise la stratégie de conservation ILM.
 - Après 50 jours, un marqueur de suppression est créé et « vidéo/film » devient non courant.
 - Après 20 jours, un total de 70 jours depuis l'entrée, "vidéo/film" est supprimé.
 - Après 30 jours, soit un total de 100 jours depuis l'entrée et de 50 jours depuis la création du marqueur de suppression, le marqueur de suppression périmé est supprimé.

Exemple de cycle de vie de compartiment permettant implicitement de conserver indéfiniment

Politique ILM

- Règle basée sur une référence d'heure non courante : au jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence d'heure d'entrée (par défaut) : au jour 0, conserver X copies pendant 50 jours

Cycle de vie du godet

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Elle correspond au filtre de cycle de vie du compartiment du préfixe « docs/ ».

L'`Expiration` action ne s'applique qu'aux marqueurs de suppression expirés, ce qui implique de conserver tout le reste indéfiniment (en commençant par "docs/").

Les marqueurs de suppression commençant par « docs/ » sont supprimés lorsqu'ils sont expirés.

- Un objet nommé « vidéo/film » est ingéré. Elle ne correspond pas au filtre et utilise la stratégie de conservation ILM.
 - Après 50 jours, un marqueur de suppression est créé et « vidéo/film » devient non courant.
 - Après 20 jours, un total de 70 jours depuis l'entrée, "vidéo/film" est supprimé.
 - Après 30 jours, soit un total de 100 jours depuis l'entrée et de 50 jours depuis la création du marqueur de suppression, le marqueur de suppression périmé est supprimé.

Exemple d'utilisation du cycle de vie du compartiment pour dupliquer la règle ILM et nettoyer les marqueurs de suppression expirés

Politique ILM

- Règle basée sur une référence d'heure non courante : au jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence d'heure d'ingestion (par défaut) : au jour 0, conserver X copies indéfiniment

Cycle de vie du godet

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Résultat

- La règle ILM est dupliquée tout au long du cycle de vie du compartiment.
 - La règle permanente de la règle ILM permet de supprimer les objets manuellement et de nettoyer les versions non actuelles au bout de 20 jours. Par conséquent, la règle de temps d'entrée conserve indéfiniment les marqueurs de suppression expirés.
 - Le cycle de vie du compartiment duplique le comportement de la règle ILM lors de l'ajout de "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 compartiment 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 est mis à jour.
 - Au bout de 20 jours, l'objet non courant est supprimé et le marqueur de suppression a expiré.
 - Peu de temps après, le marqueur de suppression périmé est supprimé.

Renforcement du système pour StorageGRID

Découvrez le renforcement du système pour StorageGRID

Le renforcement des systèmes consiste à éliminer autant de risques que possible pour la sécurité d'un système StorageGRID.

Lors de l'installation et de la configuration de StorageGRID, suivez 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. Ces meilleures pratiques doivent inclure la sécurité physique et environnementale qui limite l'accès physique et protège le centre de données physique et

l'infrastructure de support. Vous devez également vous référer à toutes les normes et recommandations réglementaires applicables à votre entreprise et à votre zone géographique.

StorageGRID suit le "[Politique de gestion des vulnérabilités de NetApp](#)". Toutes les vulnérabilités signalées sont vérifiées et traitées selon le processus de réponse aux incidents de sécurité.

Lors du renforcement d'un système StorageGRID, tenez compte des points suivants :

- **Lequel des trois réseaux StorageGRID** que vous avez mis en œuvre. Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau Admin, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- **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 conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme dispose de son propre ensemble de meilleures pratiques en matière de renforcement.
- **Comment les comptes de locataires sont approuvés.** Si vous êtes un fournisseur de services avec des comptes de locataires non fiables, vous vous interrogez différemment que si vous utilisez uniquement des locataires internes fiables.
- **Les exigences et conventions de sécurité** que votre organisation suit. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Recommandations de renforcement pour les mises à niveau logicielles StorageGRID

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous protéger contre les attaques.

Mises à niveau du logiciel StorageGRID

Dans la mesure du possible, vous devez mettre à niveau le logiciel StorageGRID vers la version principale la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire le temps d'activation des vulnérabilités connues et de réduire la surface d'attaque globale. En outre, les versions les plus récentes de StorageGRID comprennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

Consultez le "[Matrice d'interopérabilité NetApp](#)" (IMT) pour déterminer quelle version du logiciel StorageGRID vous devez utiliser. Lorsqu'un correctif est requis, NetApp privilégie la création de mises à jour pour les dernières versions. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs StorageGRID les plus récents, rendez-vous sur "[Téléchargement NetApp : StorageGRID](#)".
- Pour mettre à niveau le logiciel StorageGRID, reportez-vous au "[instructions de mise à niveau](#)".
- Pour appliquer un correctif, consultez le "[Procédure de correctif StorageGRID](#)".

Mises à niveau vers des services externes

Les services externes peuvent présenter des vulnérabilités qui affectent StorageGRID indirectement. Assurez-vous que les services dont dépend StorageGRID sont maintenus à jour. Ces services incluent LDAP, KMS (ou serveur KMIP), DNS et NTP.

Pour obtenir la liste des versions prises en charge, reportez-vous au "[Matrice d'interopérabilité NetApp](#)".

Mises à niveau vers les hyperviseurs

Si vos nœuds StorageGRID s'exécutent sur VMware ou sur un autre hyperviseur, vous devez vous assurer que le logiciel et le firmware de l'hyperviseur sont à jour.

Pour obtenir la liste des versions prises en charge, reportez-vous au ["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 de noyau sont appliquées au système d'exploitation hôte. En outre, vous devez appliquer des mises à jour de micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Pour obtenir la liste des versions prises en charge, reportez-vous au ["Matrice d'interopérabilité NetApp"](#).

Instructions de renforcement des réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur les réseaux StorageGRID, reportez-vous au ["Types de réseau StorageGRID"](#).

Instructions relatives au réseau Grid

Vous devez configurer un réseau Grid pour tout le trafic StorageGRID interne. Tous les nœuds de la grille se trouvent sur le réseau Grid et ils doivent pouvoir communiquer avec tous les autres nœuds.

Lors de la configuration du réseau Grid, suivez les instructions suivantes :

- Assurez-vous que le réseau est sécurisé par des clients non approuvés, tels que ceux qui se trouvent sur Internet ouvert.
- Si possible, utilisez le réseau Grid exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent d'autres restrictions de pare-feu qui bloquent le trafic externe vers les services internes. L'utilisation du réseau Grid pour le trafic client externe est prise en charge, mais cette utilisation offre moins de couches de protection.
- Si le déploiement StorageGRID s'étend sur plusieurs data centers, utilisez un réseau privé virtuel (VPN) ou un équivalent sur le réseau Grid afin de protéger le trafic interne.
- Certaines procédures de maintenance exigent un accès SSH (Secure Shell) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds de la grille. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients approuvés.

Instructions pour le réseau d'administration

Le réseau Admin est généralement utilisé pour les tâches d'administration (employés de confiance utilisant Grid Manager ou SSH) et pour la communication avec d'autres services de confiance tels que LDAP, DNS, NTP, KMS (ou serveur KMIP). Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau Admin, suivez les instructions suivantes :

- Bloquez tous les ports de trafic internes sur le réseau d'administration. Voir la ["liste des ports internes"](#).
- Si des clients non approuvés peuvent accéder au réseau d'administration, bloquez l'accès à StorageGRID

sur le réseau d'administration avec un pare-feu externe.

Directives pour le réseau client

Le réseau client est généralement utilisé pour les locataires et pour communiquer avec des services externes, tels que le service de réplication CloudMirror ou un autre service de plate-forme. Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez les instructions suivantes :

- Bloquer tous les ports de trafic interne sur le réseau client. Voir la ["liste des ports internes"](#).
- Acceptez le trafic client entrant uniquement sur les terminaux configurés explicitement. Voir les informations sur ["gestion des contrôles de pare-feu"](#).

Instructions de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud dispose de ses propres pratiques de renforcement.

Contrôler l'accès IPMI à distance au BMC

Vous pouvez activer ou désactiver l'accès IPMI distant pour tous les équipements contenant un BMC. L'interface IPMI distante permet à toute personne disposant d'un compte BMC et d'un mot de passe d'accéder au matériel de bas niveau de vos équipements StorageGRID. Si vous n'avez pas besoin d'accès IPMI distant au BMC, désactivez cette option.

- Pour contrôler l'accès IPMI distant au BMC dans Grid Manager, accédez à **Configuration > Security > Security settings > Appliances > Remote IPMI access** :
 - Décochez la case **Activer l'accès IPMI distant** pour désactiver l'accès IPMI au contrôleur BMC.
 - Cochez la case **Activer l'accès IPMI distant** pour activer l'accès IPMI au contrôleur BMC.

Pour plus d'informations sur le renforcement du BMC , consultez le ["Contrôleurs de gestion de la carte mère Harden"](#) fiche d'information sur la cybersécurité du ["Agence de sécurité nationale \(NSA\)"](#) et ["Agence de cybersécurité et de sécurité des infrastructures \(CISA\)"](#) .

Modifier le mot de passe BMC de l'appliance

Vous pouvez modifier le mot de passe BMC d'un appareil pour limiter l'accès et améliorer la sécurité du système.

1. Dans Grid Manager, accédez à **Nœuds > grid node > Paramètres BMC**.
2. Dans la section **Changer le mot de passe**, saisissez un nouveau mot de passe BMC de 8 à 16 caractères dans **Nouveau mot de passe**, puis saisissez-le à nouveau dans **Confirmer le nouveau mot de passe**.
3. Sélectionnez **Enregistrer**.

Vous pouvez également changer le mot de passe BMC à l'aide de l'`PUT /bmc-configuration/root-password`API.

Contrôlez l'accès aux ports USB externes des appliances

Vous pouvez activer les ports USB des appliances pour permettre au support technique d'accéder aux ports à des fins de diagnostic et de dépannage. Si vous n'avez pas besoin d'accéder aux ports USB, désactivez les ports pour des raisons de sécurité. Les ports USB sont activés par défaut après l'installation initiale ou une mise à niveau.

- Dans Grid Manager, accédez à **Configuration > Sécurité > Paramètres de sécurité > Appareils > Accès aux ports USB** pour activer ou désactiver les ports USB :

- Cochez la case **Activer les ports USB** et enregistrez pour activer les ports.

Si la case USB a été précédemment décochée et enregistrée, cochez la case **Activer les ports USB** et enregistrez pour activer de nouveau les ports USB.

- Décochez la case **Activer les ports USB** et enregistrez pour désactiver les ports.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez examiner les configurations de pare-feu externes et les modifier afin que le trafic soit accepté uniquement à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Vous devez "[gérer les contrôles de pare-feu internes](#)" empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grid spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Plus précisément, vous pouvez gérer les domaines suivants :

- **Adresses privilégiées** : vous pouvez autoriser certaines adresses IP ou sous-réseaux à accéder aux ports fermés par les paramètres de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : vous pouvez fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client ainsi que les ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non approuvé est configuré.

Bien que ce pare-feu interne offre une couche supplémentaire de protection contre certaines menaces courantes, il ne supprime pas la nécessité d'un pare-feu externe.

Pour une liste de tous les ports internes et externes utilisés par StorageGRID, voir "[Ports internes StorageGRID](#)" et "[Ports utilisés pour les communications externes](#)".

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 les logiciels non fiables. Ne supposez pas que les protections de l'hyperviseur empêchent les logiciels malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le logiciel malveillant existent sur le même matériel physique. Par exemple, les attaques Meltdown et Specter exploitent des vulnérabilités critiques dans les processeurs modernes et permettent aux programmes de voler des données en mémoire sur le même ordinateur.

Protéger les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID sur le réseau lors de l'installation des nœuds. Les nœuds ne sont pas entièrement sécurisés tant qu'ils n'ont pas rejoint la grille.

Limiter l'accès physique au matériel

Vous devez limiter l'accès physique aux nœuds de l'appliance matérielle StorageGRID ainsi qu'aux hôtes de machines virtuelles VMware et aux hôtes Linux exécutant StorageGRID aux seuls administrateurs autorisés. Certains exemples de contrôles d'accès physiques comprennent les serrures, les gardes, les barrières physiques et la vidéosurveillance.

Les nœuds d'appareils matériels sont conçus pour être installés et exploités uniquement par des administrateurs autorisés. N'autorisez pas les administrateurs non autorisés à accéder aux nœuds de l'appliance matérielle.

Instructions pour les nœuds d'administration

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un nœud d'administration.

Suivez les instructions suivantes pour sécuriser les nœuds d'administration dans votre système StorageGRID :

- Sécurisez tous les nœuds d'administration des clients non fiables, tels que ceux qui sont sur Internet ouvert. Assurez-vous qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau Grid, le réseau d'administration ou le réseau client.
- Les groupes StorageGRID contrôlent l'accès aux fonctionnalités de Grid Manager et de tenant Manager. Accordez à chaque groupe d'utilisateurs les autorisations minimales requises pour leur rôle et utilisez le mode d'accès en lecture seule pour empêcher les utilisateurs de modifier la configuration.
- Lorsque vous utilisez des terminaux d'équilibrage de charge StorageGRID, utilisez des nœuds de passerelle au lieu des nœuds d'administration pour le trafic client non fiable.
- Si vous avez des locataires non approuvés, ne les autorisez pas à avoir un accès direct au gestionnaire de locataires ou à l'API de gestion des locataires. Certains locataires non fiables utilisent un portail de locataires ou un système de gestion externe des locataires qui interagit avec l'API de gestion des locataires.
- Vous pouvez également utiliser un proxy d'administration pour davantage de contrôle sur la communication AutoSupport entre les nœuds d'administration et le support NetApp. Voir les étapes pour ["création d'un proxy d'administration"](#).
- Utilisez éventuellement les ports 8443 et 9443 restreints pour séparer les communications Grid Manager et tenant Manager. Bloquez le port partagé 443 et limitez les demandes des locataires au port 9443 pour une protection supplémentaire.
- La possibilité d'utiliser des nœuds d'administration distincts pour les administrateurs du grid et les

utilisateurs des locataires.

Pour plus d'informations, reportez-vous aux instructions "[Administration d'StorageGRID](#)" de .

Consignes relatives aux nœuds de stockage

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Suivez ces instructions pour sécuriser les nœuds de stockage dans votre système StorageGRID.

- N'autorisez pas les clients non fiables 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 du compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser son propre référentiel d'identité et n'autorisez pas l'utilisation des services de plate-forme. Voir les étapes pour "[création d'un compte de locataire](#)".
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour davantage de contrôle sur les pools de stockage cloud et la communication des services de plateforme depuis les 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.

Instructions pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de la charge facultative que les applications client peuvent utiliser pour se connecter à StorageGRID. Pour sécuriser tous les nœuds de passerelle de votre système StorageGRID, procédez comme suit :

- Configurez et utilisez des terminaux d'équilibrage de charge. Voir "[Considérations relatives à l'équilibrage de charge](#)".
- Utilisez un équilibreur de charge tiers entre le client et le nœud de passerelle ou les nœuds de stockage pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut, éventuellement, être configuré de manière à passer par un terminal interne d'équilibrage de la charge ou être directement envoyé aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, 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.

Consignes pour les nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour une utilisation dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. Les autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds de passerelle. Vous pouvez associer des nœuds d'appliance à des nœuds basés sur logiciel ou déployer des grilles 100 % appliance entièrement

conçues.

Pour sécuriser les nœuds d'appliance matérielle de votre système StorageGRID, procédez comme suit :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non fiables d'accéder à SANtricity System Manager sur le réseau.
- Si l'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.

Vous pouvez établir un VLAN pour isoler les connexions réseau BMC et restreindre l'accès Internet BMC aux réseaux approuvés. Pour plus d'informations sur l'application de la séparation VLAN, consultez le ["Contrôleurs de gestion de la carte mère Harden"](#) fiche d'information sur la cybersécurité du ["Agence de sécurité nationale \(NSA\)"](#) et ["Agence de cybersécurité et de sécurité des infrastructures \(CISA\)"](#).

Si un réseau de gestion interne sécurisé et fiable n'est pas disponible, laissez le port de gestion BMC déconnecté ou bloqué. Le support technique peut demander un accès temporaire pendant une demande d'assistance.

- Si l'appliance prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme IPMI (Intelligent Platform Management interface), bloquez le trafic non fiable sur le port 623.

Vous pouvez également [désactiver l'accès IPMI à distance](#).



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'appliance contenant des disques SED, FDE ou NL-SAS FIPS que vous gérez avec SANtricity System Manager ["Activez et configurez la sécurité des lecteurs SANtricity"](#).
- 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, ["Activez et configurez le chiffrement de lecteur StorageGRID"](#).
- Pour les appareils sans lecteurs SED, FDE ou FIPS, utilisez un serveur de gestion de clés (KMS) pour ["activer et configurer le chiffrement du nœud logiciel StorageGRID"](#).

Informations associées

["En savoir plus sur la sécurité des lecteurs dans SANtricity System Manager"](#)

Recommandations de renforcement pour TLS et SSH dans StorageGRID

Vous devez contrôler l'accès SSH, remplacer les certificats TLS par défaut 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 au Web StorageGRID n'est pas conforme à leurs politiques de sécurité de l'information. Sur les systèmes de production, vous devez installer un certificat numérique signé par une autorité de certification pour l'authentification de StorageGRID.

Plus précisément, vous devez utiliser des certificats de serveur personnalisés au lieu de ces certificats par défaut :

- **Certificat d'interface de gestion** : utilisé pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management.
- **Certificat API S3** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications clientes S3 utilisent pour télécharger et télécharger des données d'objet.

Voir "[Gérer les certificats de sécurité](#)" pour plus de détails et d'instructions.



StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer les certificats d'équilibreur de charge, reportez-vous à "[Configurer les terminaux de l'équilibreur de charge](#)" la section .

Lorsque vous utilisez des certificats de serveur personnalisés, suivez les instructions suivantes :

- Les certificats doivent avoir un `subjectAltName` qui correspond aux entrées DNS pour StorageGRID. Pour plus de détails, reportez-vous à la section 4.2.1.6, « Nom alternatif du sujet », dans "[RFC 5280 : certificat PKIX et profil CRL](#)".
- Si possible, évitez d'utiliser des certificats génériques. À l'exception de cette règle, le certificat d'un terminal de type hébergement virtuel S3 nécessite l'utilisation d'un caractère générique si les noms de compartiment ne sont pas connus à l'avance.
- Lorsque vous devez utiliser des caractères génériques dans les certificats, vous devez prendre des mesures supplémentaires pour réduire les risques. Utilisez un modèle générique tel que `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour d'autres applications. Ce schéma fonctionne également avec l'accès S3 de style chemin d'accès, tel que `dc1-s1.s3.example.com/mybucket`.
- Définissez les délais d'expiration du certificat sur court (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

En outre, les clients doivent utiliser un contrôle strict du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement pour les règles TLS et SSH

Vous pouvez sélectionner une stratégie de sécurité pour déterminer quels protocoles et chiffrements sont utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La 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, à la norme FIPS 140-2 ou si vous devez utiliser d'autres chiffrements.

Voir "[Gestion des règles TLS et SSH](#)" pour plus de détails et d'instructions.

Gérer l'accès SSH externe

Pour améliorer la sécurité du système, l'accès SSH externe est bloqué par défaut. Activez l'accès SSH uniquement lorsque vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage. Se référer à "[Gérer l'accès SSH externe](#)" pour plus de détails et d'instructions.

Recommandations de renforcement pour les journaux, les mots de passe et les messages d'audit dans StorageGRID

Outre les directives de renforcement des réseaux et nœuds StorageGRID, vous devez suivre les instructions de renforcement correspondant à d'autres domaines du système StorageGRID.

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 temporaire du programme d'installation dans l'interface utilisateur d'installation de StorageGRID ou dans l'API d'installation. Lorsqu'il est 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` le script.

Pour plus d'informations, se reporter à :

- "[Installer StorageGRID sur des nœuds logiciels](#)"
- "[Installez 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. En outre, les informations figurant dans les journaux StorageGRID et dans les résultats des messages d'audit sont généralement sensibles.

Configurez StorageGRID pour envoyer des événements de sécurité à un serveur syslog externe. Si vous utilisez syslog export, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Pour plus d'informations sur les journaux StorageGRID, reportez-vous à la section "[Référence des fichiers journaux](#)". Pour plus d'informations sur les messages d'audit StorageGRID, reportez-vous à la section "[Messages d'audit](#)".

NetApp AutoSupport

La fonctionnalité AutoSupport de StorageGRID vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des packages sur le site de support NetApp, l'équipe de support interne de votre entreprise ou 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 accélère l'identification et la résolution des problèmes sur le système StorageGRID.

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison de la nature sensible des packages AutoSupport, NetApp recommande vivement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des packages AutoSupport à NetApp.

Partage des ressources d'origine croisée (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines. En général, n'activez pas les codes de commande à moins qu'ils ne soient requis. Si CORS est requis, limitez-le aux origines de confiance.

Voir les étapes pour "[configuration de CORS pour les buckets et les objets](#)".

Dispositifs de sécurité externes

Une solution de renforcement complète doit traiter des mécanismes de sécurité en dehors de StorageGRID. L'utilisation de dispositifs d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID constitue un moyen efficace d'établir et de maintenir un niveau de sécurité strict. Ces systèmes de sécurité externes comprennent des pare-feu, des systèmes de prévention des intrusions (IDS) et d'autres dispositifs de sécurité.

Un équilibreur de charge tiers est recommandé pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.

Réduction des ransomwares

Protégez vos données d'objet contre les attaques par ransomware en suivant les recommandations de la section "[Protégez vos données contre les ransomwares avec StorageGRID](#)".

StorageGRID avec FabricPool

Flux de configuration pour l'utilisation de StorageGRID avec FabricPool

Si vous utilisez le logiciel NetApp ONTAP, vous pouvez utiliser NetApp FabricPool pour effectuer le Tiering des données inactives vers un système de stockage objet NetApp StorageGRID.

Suivez ces instructions pour :

- Découvrez les points à prendre en compte et les bonnes pratiques pour configurer StorageGRID pour une charge de travail FabricPool.
- Découvrez comment configurer un système de stockage objet StorageGRID à utiliser avec FabricPool.
- Découvrez comment fournir les valeurs requises à ONTAP lorsque StorageGRID est attaché à un Tier cloud FabricPool.

Démarrage rapide de la configuration de StorageGRID pour FabricPool

1

Planification de la configuration

- Déterminez quelle règle de Tiering des volumes FabricPool vous utiliserez pour effectuer le Tiering des données ONTAP inactives vers StorageGRID.
- Planifiez et installez un système StorageGRID pour répondre à vos besoins en capacité de stockage et en performances.
- Familiarisez-vous avec le logiciel système StorageGRID, y compris le "[Gestionnaire de grille](#)" et le "[Gestionnaire de locataires](#)".

- Consultez les meilleures pratiques FabricPool pour "[Groupes HAUTE DISPONIBILITÉ](#)", "[équilibrage de la charge](#)", "[ILM](#)" et "[plus encore](#)".
- Consultez les ressources supplémentaires suivantes, qui contiennent des informations détaillées sur l'utilisation et la configuration de ONTAP et FabricPool :

["Tr-4598 : meilleures pratiques FabricPool dans ONTAP"](#)

["Documentation ONTAP pour FabricPool"](#)

2

Effectuer des tâches préalables

Obtenir le "[Informations requises pour associer StorageGRID en tant que Tier cloud](#)", y compris :

- Adresses IP
- Noms de domaine
- Certificat SSL

En option, configurez "[fédération des identités](#)" et "[authentification unique](#)".

3

Configurer les paramètres StorageGRID

Utilisez StorageGRID pour obtenir les valeurs dont ONTAP a besoin pour se connecter à la grille.

L'utilisation du "[Assistant d'installation FabricPool](#)" est la méthode recommandée et la 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 "[ajoutez un tier de cloud](#)" utiliser les valeurs StorageGRID. Ensuite, "[Configurer les entrées DNS](#)" pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

5

Contrôler et gérer

Une fois votre système opérationnel, vous pouvez effectuer des tâches continues dans ONTAP et StorageGRID afin de gérer et de surveiller le Tiering des données FabricPool au fil du temps.

Qu'est-ce que FabricPool ?

FabricPool est une solution de stockage hybride ONTAP qui utilise un agrégat Flash haute performance comme Tier de performance et un magasin d'objets comme Tier cloud. Les agrégats compatibles FabricPool vous permettent de réduire les coûts de stockage sans nuire aux performances, à l'efficacité ou à la protection.

FabricPool associe un niveau cloud (un magasin d'objets externe tel que StorageGRID) à un niveau local (un agrégat de stockage ONTAP) pour créer une collection composite de disques. Les volumes dans FabricPool peuvent ensuite exploiter le Tiering en conservant les données actives dans un stockage haute performance (Tier local) et en inactivant les données inactives vers le magasin d'objets externe (Tier cloud).

Aucune modification de l'architecture n'est requise. Vous pouvez continuer à gérer vos données et votre

environnement applicatif à partir du système de stockage ONTAP central.

Qu'est-ce que StorageGRID ?

NetApp StorageGRID est une architecture de stockage qui gère les données en tant qu'objets, contrairement aux autres architectures de stockage telles que le stockage en mode bloc ou fichier. Les objets sont conservés dans un seul conteneur (tel qu'un compartiment) et ne sont pas imbriqués en tant que fichiers dans un répertoire à l'intérieur d'autres répertoires. Le stockage objet offre généralement des performances moins élevées que le stockage en mode bloc ou fichier, mais il présente aussi l'évolutivité la plus remarquable. Les compartiments StorageGRID peuvent contenir des pétaoctets de données et des milliards d'objets.

Pourquoi utiliser StorageGRID comme Tier cloud FabricPool ?

FabricPool peut hiérarchiser les données ONTAP avec plusieurs fournisseurs de stockage objet, y compris StorageGRID. Contrairement aux clouds publics qui peuvent fixer un nombre maximal d'opérations d'entrée/sortie par seconde (IOPS) pris en charge au niveau du compartiment ou du conteneur, les performances StorageGRID évoluent en fonction du nombre de nœuds qu'un système permet. En utilisant StorageGRID comme Tier cloud FabricPool, vous pouvez conserver vos données inactives dans votre propre cloud privé et bénéficier d'une performance optimale et d'un contrôle total sur vos données.

En outre, vous n'avez pas besoin d'une licence FabricPool lorsque vous utilisez StorageGRID en tant que Tier cloud.

Informations nécessaires pour connecter StorageGRID en tant que niveau cloud FabricPool

Avant de connecter StorageGRID en tant que niveau cloud pour FabricPool, vous devez effectuer les étapes de configuration dans StorageGRID et obtenir certaines valeurs à utiliser dans ONTAP.

Quelles valeurs ai-je besoin ?

Le tableau suivant indique les valeurs que vous devez configurer dans StorageGRID et la manière dont ces valeurs sont utilisées par ONTAP et le serveur DNS.

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Adresses IP virtuelles (VIP)	Groupe StorageGRID > HA	Entrée DNS
Port	StorageGRID > terminal de l'équilibreur de charge	ONTAP System Manager > Ajouter un Tier cloud
Certificat SSL	StorageGRID > terminal de l'équilibreur de charge	ONTAP System Manager > Ajouter un Tier cloud
Nom du serveur (FQDN)	StorageGRID > terminal de l'équilibreur de charge	Entrée DNS
ID de clé d'accès et clé d'accès secrète	StorageGRID > locataire et compartiment	ONTAP System Manager > Ajouter un Tier cloud

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Nom du compartiment/conteneur	StorageGRID > locataire et compartiment	ONTAP System Manager > Ajouter un Tier cloud

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez effectuer l'une des opérations suivantes pour obtenir les informations dont vous avez besoin :

- Utilisez le ["Assistant d'installation FabricPool"](#). L'assistant d'installation FabricPool vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un fichier que vous pouvez utiliser pour configurer ONTAP System Manager. Cet assistant vous guide tout au long des étapes requises et vous aide à vous assurer que vos paramètres sont conformes aux meilleures pratiques StorageGRID et FabricPool.
- Configurez chaque élément manuellement. Entrez ensuite les valeurs dans ONTAP System Manager ou dans l'interface de ligne de commandes ONTAP. Voici la procédure à suivre :
 - a. ["Configurez un groupe haute disponibilité pour FabricPool"](#).
 - b. ["Créez un noeud final d'équilibrage de charge pour FabricPool"](#).
 - c. ["Créez un compte de locataire pour FabricPool"](#).
 - d. Connectez-vous au compte du locataire, et ["créez le compartiment et les clés d'accès pour l'utilisateur root"](#).
 - e. Créez une règle ILM pour les données FabricPool et ajoutez-la à vos règles ILM actives. Voir ["Configurez la solution ILM pour les données FabricPool"](#).
 - f. En option, ["Créez une stratégie de classification du trafic pour FabricPool"](#).

Utilisez l'assistant d'installation FabricPool

Découvrez l'assistant de configuration FabricPool de StorageGRID

Vous pouvez utiliser l'assistant d'installation de FabricPool pour configurer StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool. Une fois l'assistant d'installation terminé, vous pouvez entrer les informations requises dans ONTAP System Manager.

Quand utiliser l'assistant de configuration FabricPool

L'assistant d'installation FabricPool vous guide à chaque étape de la configuration de StorageGRID pour une utilisation avec FabricPool et configure automatiquement certaines entités pour vous, telles que les règles ILM et de classification du trafic. Dans le cadre de l'assistant, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux meilleures pratiques StorageGRID et FabricPool.

En supposant que vous disposez de l'autorisation d'accès racine, vous pouvez exécuter l'assistant de configuration FabricPool lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement. En fonction de vos besoins, vous pouvez également configurer manuellement une partie ou la totalité des éléments requis, puis utiliser l'assistant pour assembler les valeurs dont ONTAP a besoin dans un seul fichier.



Utilisez l'assistant d'installation de FabricPool, sauf si vous savez que vous avez des exigences spéciales, sinon votre implémentation nécessitera une personnalisation importante.

Avant d'utiliser l'assistant

Confirmez que vous avez effectué ces étapes préalables.

Passez en revue les bonnes pratiques

- Vous avez une compréhension générale de la ["Informations requises pour associer StorageGRID en tant que Tier cloud"](#).
- Vous avez examiné les bonnes pratiques de FabricPool pour :
 - ["Groupes haute disponibilité \(HA\)"](#)
 - ["Équilibrage de la charge"](#)
 - ["Règles et règles ILM"](#)

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité, vous savez à quels nœuds ONTAP se connectera et à quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs entrer pour le CIDR de sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour isoler le trafic FabricPool, vous avez déjà configuré l'interface VLAN. Voir ["Configurez les interfaces VLAN"](#).

Configurer la fédération des identités et SSO

Si vous prévoyez d'utiliser la fédération 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 des identités"](#) et ["Configurer l'authentification unique"](#).

Obtenir et configurer des noms de domaine

- Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées de serveur de noms de domaine (DNS) mapperont ce FQDN aux adresses IP virtuelles (VIP) du groupe haute disponibilité que vous créez à l'aide de l'assistant. Voir ["Configurer le serveur DNS"](#).
- Si vous prévoyez d'utiliser des requêtes S3 de type hébergement virtuel, vous avez ["Noms de domaine de terminaux S3 configurés"](#). ONTAP utilise par défaut des URL de type chemin, mais il est recommandé d'utiliser des requêtes de type hébergement virtuel.

Examinez les exigences en matière d'équilibreur de charge et de certificat de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID, vous avez examiné le document général ["considérations relatives à l'équilibrage de charge"](#). Vous disposez des certificats que vous allez télécharger ou des valeurs dont vous avez besoin pour générer un certificat.

Si vous prévoyez d'utiliser un nœud final externe (tiers) d'équilibreur de charge, vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Confirmation de la configuration du pool de stockage ILM

Si vous avez 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 des données ONTAP.



Cette condition préalable ne s'applique pas si vous avez installé StorageGRID 11.7 ou 11.8. Lors de l'installation initiale de l'une de ces versions, les pools de stockage sont automatiquement créés pour chaque site.

Relation entre ONTAP et le niveau cloud StorageGRID

L'assistant FabricPool vous guide tout au long du processus de création d'un niveau cloud StorageGRID unique, qui inclut un locataire StorageGRID, un ensemble de clés d'accès et un compartiment StorageGRID. Vous pouvez associer ce niveau cloud StorageGRID à un ou plusieurs niveaux locaux ONTAP.

L'association d'un seul niveau de cloud à plusieurs niveaux locaux dans un cluster est la meilleure pratique générale. Cependant, selon vos besoins, vous pouvez utiliser plusieurs compartiments, voire plus d'un locataire StorageGRID pour les niveaux locaux dans un seul cluster. L'utilisation de différents compartiments et locataires vous permet d'isoler les données et l'accès aux données entre les tiers locaux ONTAP, mais sa configuration et sa gestion sont un peu plus complexes.

NetApp déconseille d'associer un seul Tier cloud à des tiers locaux dans plusieurs clusters.



Pour connaître les meilleures pratiques d'utilisation de StorageGRID avec NetApp MetroCluster™ et FabricPool Mirror, voir ["Tr-4598 : meilleures pratiques FabricPool dans ONTAP"](#).

Facultatif : utilisez un compartiment différent pour chaque niveau local

Pour utiliser plusieurs compartiments pour les tiers locaux d'un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque Tier cloud partage le même groupe haute disponibilité, mais il utilise un conteneur différent (compartiment StorageGRID) pour le terminal de l'équilibreur de charge, le locataire et les clés d'accès. Procédez comme suit :

1. Dans StorageGRID Grid Manager, suivez les instructions de l'assistant d'installation FabricPool pour le premier niveau cloud.
2. Dans ONTAP System Manager, ajoutez un Tier cloud et utilisez le fichier téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Dans le gestionnaire de locataires StorageGRID, connectez-vous au locataire créé par l'assistant, puis créez un second compartiment.
4. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe haute disponibilité, le terminal de l'équilibreur de charge et le locataire existants. Sélectionnez ensuite le nouveau compartiment que vous avez créé manuellement. Créez une règle ILM pour le nouveau compartiment et activez une règle ILM pour inclure cette règle.
5. Depuis ONTAP, ajoutez un second Tier cloud, mais indiquez le nouveau nom de compartiment.

Facultatif : utilisez un locataire et un compartiment différents pour chaque niveau local

Pour utiliser plusieurs locataires et jeux de clés d'accès différents pour les tiers locaux d'un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque Tier cloud partage le même groupe haute disponibilité et le même terminal d'équilibrage de la charge, mais utilise un locataire, des clés d'accès et un

conteneur différents (compartiment StorageGRID). Procédez comme suit :

1. Dans StorageGRID Grid Manager, suivez les instructions de l'assistant d'installation FabricPool pour le premier niveau cloud.
2. Dans ONTAP System Manager, ajoutez un Tier cloud et utilisez le fichier téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe haute disponibilité et le terminal d'équilibrage de la charge existants. Créez un locataire et un compartiment. Créez une règle ILM pour le nouveau compartiment et activez une règle ILM pour inclure cette règle.
4. Depuis ONTAP, ajoutez un second Tier cloud, mais fournissez la nouvelle clé d'accès, la clé secrète et le nom du compartiment.

Accédez à l'assistant de configuration StorageGRID FabricPool et terminez-le

Vous pouvez utiliser l'assistant d'installation de FabricPool pour configurer StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool.

Avant de commencer

- Vous avez examiné le ["considérations et exigences"](#) pour à l'aide de l'assistant d'installation de FabricPool.



Si vous souhaitez configurer StorageGRID pour une utilisation avec une autre application client S3, rendez-vous sur ["Utilisation de l'assistant d'installation S3"](#).

- Vous avez le ["Autorisation d'accès racine"](#).

Accéder à l'assistant

Vous pouvez exécuter l'assistant d'installation FabricPool lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Si la bannière **FabricPool and S3 setup wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide  dans la barre d'en-tête du Grid Manager et sélectionnez **FabricPool and S3 setup wizard**.
3. Dans la section FabricPool de la page de l'assistant d'installation de FabricPool et S3, sélectionnez **configurer maintenant**.

L'étape 1 sur 9 : configurer le groupe HA s'affiche.

Étape 1 sur 9 : configuration du groupe haute disponibilité

Un groupe haute disponibilité (HA) est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données FabricPool disponibles. Un groupe haute disponibilité utilise des adresses IP virtuelles (VIP) pour fournir un accès haute disponibilité au service Load Balancer. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool

Pour plus d'informations sur cette tâche, reportez-vous aux sections "[Gérez les groupes haute disponibilité](#)" et "[Meilleures pratiques pour les groupes à haute disponibilité](#)".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, il n'est pas nécessaire de créer un groupe haute disponibilité. Sélectionnez **Ignorer cette étape** et passez à [Étape 2 sur 9 : configuration du terminal de l'équilibreur de charge](#).
2. Pour utiliser l'équilibreur de charge StorageGRID, créez un nouveau groupe haute disponibilité ou utilisez un groupe haute disponibilité existant.

Création du groupe haute disponibilité

- a. Pour créer un nouveau groupe HA, sélectionnez **Create HA group**.
- b. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

- c. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

- d. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP repassent à l'interface de priorité la plus élevée disponible.

- e. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR—adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple 192.16.0.0/22, .
Adresse IP de la passerelle (facultative)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP et toutes seront actives en même temps sur l'interface active. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA**, puis sélectionnez **Terminer** pour revenir à l'assistant de configuration FabricPool.

g. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Utilisez un groupe haute disponibilité existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans la liste déroulante **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Étape 2 sur 9 : configuration du terminal de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir d'applications client, telles qu'FabricPool. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service StorageGRID Load Balancer, qui existe sur tous les nœuds de passerelle et d'administration, ou vous pouvez vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, reportez-vous aux sections général "[considérations relatives à l'équilibrage de charge](#)" et "[Bonnes pratiques en matière d'équilibrage de charge pour FabricPool](#)".

Étapes

1. Sélectionnez ou créez un point d'extrémité de l'équilibreur de charge StorageGRID ou utilisez un équilibreur de charge externe.

Créer un point final

- a. Sélectionnez **Créer un noeud final**.
- b. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la "Référence du port réseau".
Type de client	Doit être S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

- c. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accessible à l'aide d'une 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 final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce nœud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

d. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. Autoriser tous les locataires est presque toujours l'option appropriée pour le nœud final de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous utilisez l'assistant d'installation FabricPool pour un nouveau système StorageGRID et que vous n'avez pas encore créé de compte de locataire.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce nœud final.

e. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
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 d'API S3" pour plus de détails.

f. Sélectionnez **Terminer** pour revenir à l'assistant de configuration FabricPool.

g. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utilisez le terminal d'équilibrage de charge existant

- a. Sélectionnez le nom d'un nœud final existant dans la liste déroulante **Sélectionner un nœud final d'équilibrage de charge**.
- b. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Utiliser un équilibreur de charge externe

- a. Renseignez les champs suivants pour l'équilibreur de charge externe.

Champ	Description
FQDN	Nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que FabricPool utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

- b. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Étape 3 sur 9 : locataire et compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire dispose de ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités. Vous devez créer un locataire StorageGRID avant de pouvoir créer le compartiment que FabricPool utilisera.

Un compartiment est un conteneur utilisé pour stocker les objets d'un locataire et ses métadonnées d'objet. Même si certains locataires peuvent avoir plusieurs compartiments, l'assistant vous permet de créer ou de sélectionner un seul locataire et un compartiment à la fois. Vous pouvez utiliser le gestionnaire de locataires ultérieurement pour ajouter des compartiments supplémentaires dont vous avez besoin.

Vous pouvez créer un locataire et un compartiment pour FabricPool ou sélectionner un locataire et un compartiment existants. Si vous créez un nouveau locataire, le système crée automatiquement l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root du locataire.

Pour plus d'informations sur cette tâche, reportez-vous aux sections "[Créez un compte de locataire pour FabricPool](#)" et "[Créez un compartiment S3 et obtenez une clé d'accès](#)".

Étapes

Créez un locataire et un compartiment ou sélectionnez un locataire existant.

Nouveaux locataires et compartiments

1. Pour créer un nouveau tenant et un compartiment, entrez un **tenant name**. Par exemple `FabricPool tenant, .`
2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise "[fédération des identités](#)", "[Authentification unique \(SSO\)](#)", ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

3. Pour **nom de compartiment**, entrez le nom du compartiment que FabricPool utilisera pour stocker les données ONTAP. Par exemple `fabricpool-bucket, .`



Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

4. Sélectionnez la **région** pour ce compartiment.

Utilisez la région par défaut (`us-east-1`) à moins d'utiliser ILM à l'avenir pour filtrer des objets en fonction de la région du compartiment.

5. Sélectionnez **Créer et continuer** pour créer le tenant et le compartiment et pour accéder à l'étape de téléchargement des données

Sélectionnez locataire et compartiment

La gestion des versions du compte de locataire existant doit comporter au moins un compartiment pour lequel la gestion des versions n'est pas activée. Vous ne pouvez pas sélectionner un compte de locataire existant s'il n'existe aucun compartiment pour ce locataire.

1. Sélectionnez le locataire existant dans la liste déroulante **tenant name**.
2. Sélectionnez le compartiment existant dans la liste déroulante **Nom du compartiment**.

FabricPool ne prend pas en charge la gestion des versions d'objet, de sorte que les compartiments pour lesquels la gestion des versions est activée ne sont pas affichés.



Ne sélectionnez pas un compartiment dans lequel le verrouillage d'objet S3 est activé pour FabricPool.

3. Sélectionnez **Continuer** pour accéder à l'étape de téléchargement des données.

Étape 4 sur 9 : télécharger les paramètres ONTAP

Au cours de cette étape, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager.

Étapes

1. Vous pouvez également sélectionner l'icône de copie () pour copier à la fois l'ID de clé d'accès et la clé d'accès secrète dans le presse-papiers.

Ces valeurs sont incluses dans le fichier de téléchargement, mais vous pouvez les enregistrer séparément.

2. Sélectionnez **Télécharger les paramètres ONTAP** pour télécharger un fichier texte contenant les valeurs que vous avez saisies jusqu'à présent.

Il `ONTAP_FabricPool_settings_bucketname.txt` contient les informations nécessaires à la configuration de StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool, notamment :

- Détails de la connexion de l'équilibreur de charge, y compris le nom du serveur (FQDN), le port et le certificat
- Nom du compartiment
- ID de clé d'accès et clé d'accès secrète pour l'utilisateur root du compte de locataire

3. Enregistrez les clés copiées et le fichier téléchargé dans un emplacement sécurisé.



Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès, téléchargé les paramètres ONTAP ou les deux. Les touches ne seront pas disponibles après la fermeture de cette page. Veillez à enregistrer ces informations dans un emplacement sécurisé car elles peuvent être utilisées pour obtenir des données de votre système StorageGRID.

4. Cochez la case pour confirmer que vous avez téléchargé ou copié l'ID de clé d'accès et la clé d'accès secrète.
5. Sélectionnez **Continuer** pour accéder à l'étape du pool de stockage ILM.

Étape 5 sur 9 : sélectionnez un pool de stockage

Un pool de stockage est un groupe de nœuds de stockage. Lorsque vous sélectionnez un pool de stockage, vous déterminez les nœuds que StorageGRID utilisera pour stocker les données hiérarchisées depuis ONTAP.

Pour plus de détails sur cette étape, voir "[Créer un pool de stockage](#)".

Étapes

1. Dans la liste déroulante **site**, sélectionnez le site StorageGRID que vous souhaitez utiliser pour les données hiérarchisées à partir de ONTAP.
2. Dans la liste déroulante **Storage pool**, sélectionnez le pool de stockage pour ce site.

Le pool de stockage d'un site inclut tous les nœuds de stockage de ce site.

3. Sélectionnez **Continuer** pour accéder à l'étape de la règle ILM.

Étape 6 sur 9 : révision de la règle ILM pour FabricPool

Les règles de gestion du cycle de vie des informations (ILM) contrôlent le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID.

L'assistant d'installation de FabricPool crée automatiquement la règle ILM recommandée pour l'utilisation de FabricPool. Cette règle s'applique uniquement au compartiment spécifié. Elle stocke les données hiérarchisées depuis ONTAP en utilisant un code d'effacement 2+1 sur un même site.

Pour plus de détails sur cette étape, voir ["Création d'une règle ILM"](#) et ["Bonnes pratiques d'utilisation d'ILM avec des données FabricPool"](#).

Étapes

1. Vérifiez les détails de la règle.

Champ	Description
Nom de la règle	Généré automatiquement et ne pouvant pas être modifié
Description	Généré automatiquement et ne pouvant pas être modifié
Filtre	Nom du compartiment Cette règle s'applique uniquement aux objets enregistrés dans le compartiment spécifié.
Heure de référence	Temps d'ingestion L'instruction de placement démarre lorsque les objets sont initialement enregistrés dans le compartiment.
Instruction de placement	Utilisez le code d'effacement 2+1

2. Triez le diagramme de rétention par **période** et **pool de stockage** pour confirmer l'instruction de placement.
 - La **période** pour la règle est **jour 0 - pour toujours**. **Jour 0** signifie que la règle est appliquée lorsque les données sont hiérarchisées depuis ONTAP. **Forever** signifie que l'ILM de StorageGRID ne supprimera pas les données qui ont été hiérarchisées depuis ONTAP.
 - Le **pool de stockage** de la règle est le pool de stockage que vous avez sélectionné. **EC 2+1** signifie que les données seront stockées à l'aide du code d'effacement 2+1. Chaque objet sera enregistré sous forme de deux fragments de données et d'un fragment de parité. Les trois fragments de chaque objet seront enregistrés sur différents nœuds de stockage sur un seul site.
3. Sélectionnez **Créer et continuer** pour créer cette règle et accéder à l'étape de la stratégie ILM.

Étape 7 sur 9 : vérification et activation de la règle ILM

Une fois que l'assistant d'installation de FabricPool a créé la règle ILM pour FabricPool, il crée une règle ILM. Vous devez soigneusement simuler et réviser cette stratégie avant de l'activer.

Pour plus de détails sur cette étape, voir "[Création de la règle ILM](#)" et "[Bonnes pratiques d'utilisation d'ILM avec des données FabricPool](#)".



Lorsque vous activez une nouvelle règle ILM, StorageGRID utilise cette règle pour gérer le placement, la durée et la protection des données de tous les objets de la grille, y compris les objets existants et les objets nouvellement ingérés. Dans certains cas, l'activation d'une nouvelle stratégie peut entraîner le déplacement d'objets existants vers de nouveaux emplacements.



Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

Étapes

1. Si vous le souhaitez, mettez à jour le **Nom de la stratégie** généré par le système. Par défaut, le système ajoute « + FabricPool » au nom de votre stratégie active ou inactive, mais vous pouvez fournir votre propre nom.
2. Consultez la liste des règles de la stratégie inactive.
 - Si aucune règle ILM n'est inactive dans votre grille, l'assistant crée une règle inactive en clonant votre règle active et en ajoutant la nouvelle règle en haut de la page.
 - Si la règle ILM de votre grid est déjà inactive et qu'elle utilise le même ordre et les mêmes règles que la règle ILM active, l'assistant ajoute la nouvelle règle en haut de la règle inactive.
 - Si votre stratégie inactive contient des règles différentes ou un ordre différent de celui de la stratégie active, l'assistant crée une nouvelle stratégie inactive en clonant votre stratégie active et en ajoutant la nouvelle règle au début.

3. Passez en revue l'ordre des règles dans la nouvelle stratégie 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 règle ne soient évaluées. Les objets d'autres compartiments sont placés selon les règles suivantes de la règle.

4. Consultez le diagramme de rétention pour savoir comment les différents objets seront conservés.
 - a. Sélectionnez **développer tout** pour afficher un diagramme de rétention pour chaque règle de la stratégie inactive.
 - b. Sélectionnez **Time Period** et **Storage Pool** pour consulter le diagramme de rétention. Vérifiez que toutes les règles qui s'appliquent au compartiment FabricPool ou au locataire conservent les objets **Forever**.
5. Lorsque vous avez examiné la stratégie inactive, sélectionnez **Activer et continuer** pour activer la stratégie et passer à l'étape de classification du trafic.



Les erreurs d'une règle ILM peuvent entraîner des pertes de données irréparables. Examinez attentivement la stratégie avant de l'activer.

Étape 8 de 9 : création d'une politique de classification du trafic

L'assistant d'installation FabricPool peut également créer une règle de classification du trafic que vous pouvez utiliser pour contrôler la charge de travail FabricPool. La stratégie créée par le système utilise une règle de correspondance pour identifier tout le trafic réseau lié au compartiment que vous avez créé. Cette règle surveille uniquement le trafic ; elle ne limite pas le trafic pour FabricPool ou tout autre client.

Pour plus de détails sur cette étape, voir "[Créer une règle de classification du trafic pour FabricPool](#)".

Étapes

1. Consultez la politique.
2. Si vous souhaitez créer cette stratégie de classification de trafic, sélectionnez **Créer et continuer**.

Dès que FabricPool commence à hiérarchiser les données vers StorageGRID, vous pouvez accéder à la page règles de classification du trafic pour afficher les mesures du trafic réseau correspondant à cette règle. Par la suite, vous pouvez également ajouter des règles pour limiter d'autres charges de travail et vous assurer que la charge de travail FabricPool dispose de la plus grande partie de la bande passante.

3. Sinon, sélectionnez **Ignorer cette étape**.

Étape 9 sur 9 : passez en revue le résumé

Ce récapitulatif fournit des informations détaillées sur les éléments que vous avez configurés, notamment le nom de l'équilibreur de charge, le locataire et le compartiment, la règle de classification du trafic et la règle ILM active.

Étapes

1. Passez en revue le résumé.
2. Sélectionnez **Terminer**.

Étapes suivantes

Une fois l'assistant FabricPool terminé, effectuez les étapes suivantes.

Étapes

1. Accédez à "[Configuration de ONTAP System Manager](#)" pour saisir les valeurs enregistrées et terminer le côté ONTAP de la connexion. Vous devez ajouter StorageGRID en tant que Tier cloud, relier le Tier cloud à un Tier local pour créer une FabricPool et définir des règles de Tiering des volumes.
2. Accédez à "[Configurer le serveur DNS](#)" et assurez-vous que le DNS inclut un enregistrement permettant d'associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez.
3. Consultez la section "[Autres meilleures pratiques pour StorageGRID et FabricPool](#)" pour connaître les bonnes pratiques en matière de journaux d'audit StorageGRID et d'autres options de configuration globale.

Configurez StorageGRID manuellement

Créez un groupe à haute disponibilité (HA) pour FabricPool dans StorageGRID

Lorsque vous configurez StorageGRID pour une utilisation avec FabricPool, vous pouvez éventuellement créer un ou plusieurs groupes haute disponibilité (HA). Un groupe haute disponibilité est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des

nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données FabricPool disponibles. Un groupe haute disponibilité utilise des adresses IP virtuelles (VIP) pour fournir un accès haute disponibilité au service Load Balancer. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool.

Pour plus de détails sur cette tâche, reportez-vous ["Gérez les groupes haute disponibilité"](#) à la section . Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à ["Accédez à l'assistant d'installation FabricPool et terminez-le"](#).

Avant de commencer

- Vous avez examiné le ["meilleures pratiques pour les groupes haute disponibilité"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Si vous prévoyez d'utiliser un VLAN, vous avez créé l'interface VLAN. Voir ["Configurez les interfaces VLAN"](#).

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Créer**.
3. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

4. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

5. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc.

Lorsque les pannes sont résolues, les adresses VIP repassent à l'interface de priorité la plus élevée disponible.

6. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR—adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple 192.16.0.0/22, .
Adresse IP de la passerelle (facultative)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

7. Sélectionnez **Créer groupe HA**, puis **Terminer**.

Créez un point de terminaison d'équilibrage de charge pour FabricPool dans StorageGRID

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir d'applications client, telles qu'FabricPool. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous devez configurer un point d'extrémité d'équilibreur de charge et télécharger ou générer un certificat de point d'extrémité d'équilibreur de charge, utilisé pour sécuriser la connexion entre ONTAP et StorageGRID.

Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "[Accédez à l'assistant d'installation FabricPool et terminez-le](#)".

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Autorisation d'accès racine](#)".
- Vous avez examiné le général "[considérations relatives à l'équilibrage de charge](#)" ainsi que le "[Bonnes pratiques en matière d'équilibrage de charge pour FabricPool](#)".

Étapes

1. Sélectionnez **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
2. Sélectionnez **Créer**.

3. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle. Ces ports sont réservés sur des nœuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la "Référence du port réseau". Vous fournissez ce numéro à ONTAP lorsque vous associez StorageGRID à un niveau cloud FabricPool.
Type de client	Sélectionnez S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

4. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accessible à l'aide d'une 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 final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.

Mode	Description
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

5. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. Autoriser tous les locataires est presque toujours l'option appropriée pour le nœud final de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte de locataire.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce nœud final.

6. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
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 d'API S3" pour plus de détails.

7. Sélectionnez **Créer**.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Créez un compte locataire pour FabricPool dans StorageGRID

Vous devez créer un compte de tenant dans le Grid Manager pour utilisation FabricPool.

Les comptes de locataire permettent aux applications client de stocker et de récupérer des objets sur StorageGRID. Chaque compte locataire possède son propre ID de compte, groupes et utilisateurs autorisés, compartiments et objets.

Pour plus de détails sur cette tâche, reportez-vous ["Créer un compte de locataire"](#) à la section . Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à ["Accédez à l'assistant d'installation FabricPool et terminez-le"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **Locataires**.
2. Sélectionnez **Créer**.
3. Pour les étapes entrer les détails, entrez les informations suivantes.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.
Description (facultatif)	Une description pour aider à identifier le locataire.
Type de client	Doit être S3 pour FabricPool.
Quota de stockage (facultatif)	Laissez ce champ vide pour FabricPool.

4. Pour l'étape Sélectionner les autorisations :

- a. Ne sélectionnez pas **Autoriser les services de plate-forme**.

Les locataires FabricPool n'ont généralement pas besoin d'utiliser des services de plateforme, tels que la réplication CloudMirror.

- b. Si vous le souhaitez, sélectionnez **utiliser le propre référentiel d'identité**.

- c. Ne sélectionnez pas **Autoriser la sélection S3**.

Les locataires FabricPool n'ont généralement pas besoin d'utiliser S3 Select.

- d. Vous pouvez également sélectionner **Utiliser une connexion de fédération de grille** pour permettre au locataire d'utiliser une ["connexion de fédération de grille"](#) pour la synchronisation des comptes et la réplication inter-grilles. 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 des identités"](#)

, ["Authentification unique \(SSO\)"](#) , ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

6. Sélectionnez **Créer locataire**.

Créez un compartiment S3 et obtenez les clés d'accès pour FabricPool dans StorageGRID

Avant d'utiliser StorageGRID avec un workload FabricPool, vous devez créer un compartiment S3 pour vos données FabricPool. Vous devez également obtenir une clé d'accès et une clé secrète pour le compte de locataire que vous utiliserez pour FabricPool.

Pour plus d'informations sur cette tâche, reportez-vous aux sections ["Créer un compartiment S3"](#) et ["Créez vos propres clés d'accès S3"](#). Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à ["Accédez à l'assistant d'installation FabricPool et terminez-le"](#).

Avant de commencer

- Vous avez créé un compte de locataire pour l'utilisation de FabricPool.
- Vous disposez d'un accès racine au compte de locataire.

Étapes

1. Connectez-vous au Gestionnaire de locataires.

Vous pouvez effectuer l'une des opérations suivantes :

- Dans la page comptes de tenant du Gestionnaire de grille, sélectionnez le lien **se connecter** pour le tenant et entrez vos informations d'identification.
- Saisissez l'URL du compte de tenant dans un navigateur Web et saisissez vos informations d'identification.

2. Créez un compartiment S3 pour les données FabricPool.

Vous devez créer un compartiment unique pour chaque cluster ONTAP que vous prévoyez d'utiliser.

- Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
- Sélectionnez **Créer un compartiment**.

- c. Entrez le nom du compartiment StorageGRID à utiliser avec FabricPool. Par exemple `fabricpool-bucket`, .



Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

- d. Sélectionnez la région de ce compartiment.

Par défaut, tous les buckets sont créés dans le `us-east-1` région. Si la région par défaut est configurée sur une région autre que `us-east-1`, cette autre région est initialement sélectionnée dans la liste déroulante.

- e. Sélectionnez **Continuer**.

- f. Sélectionnez **Créer un compartiment**.



Ne sélectionnez pas **Activer la gestion des versions d'objet** pour le compartiment FabricPool. De même, ne modifiez pas un compartiment FabricPool pour utiliser **disponible** ou une cohérence autre que celle par défaut. La cohérence de compartiment recommandée pour les compartiments FabricPool est **Read-After-New-write**, qui est la cohérence par défaut d'un nouveau compartiment.

3. Créez une clé d'accès et une clé d'accès secrète.

- a. Sélectionnez **STORAGE (S3) > Mes clés d'accès**.

- b. Sélectionnez **Créer clé**.

- c. Sélectionnez **Créer une clé d'accès**.

- d. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

Ces valeurs seront saisies dans ONTAP lorsque vous configurez StorageGRID en tant que Tier cloud FabricPool.



Si vous générez une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID à l'avenir, entrez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Sinon, ONTAP risque de perdre temporairement son accès à StorageGRID.

Configurer StorageGRID ILM pour les données FabricPool

Cet exemple de règle simple vous permet de commencer par vos propres règles et règles ILM.

Nous partons du principe que vous concevez les règles ILM et une règle ILM pour un système StorageGRID qui possède quatre nœuds de stockage dans un data Center unique à Denver, Colorado. Dans cet exemple, les données FabricPool utilisent un compartiment nommé `fabricpool-bucket`.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte. Pour en savoir plus, voir "[Gestion des objets avec ILM](#)".



Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

Avant de commencer

- Vous avez examiné le "[Bonnes pratiques d'utilisation d'ILM avec des données FabricPool](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Permission d'accès ILM ou racine](#)".
- Si vous avez effectué une mise à niveau vers StorageGRID 12.1 depuis une version de StorageGRID antérieure à 11.7, vous avez configuré le pool de stockage que vous utiliserez. En règle générale, vous devez créer un pool de stockage pour chaque site StorageGRID que vous utiliserez pour stocker des données. (À partir de la version 11.7, les pools de stockage sont créés automatiquement pour chaque site.)



Cette condition préalable ne s'applique pas si vous avez installé StorageGRID 11.7 ou 11.8. Lors de l'installation initiale de l'une de ces versions, les pools de stockage sont automatiquement créés pour chaque site.

Étapes

1. Créez une règle ILM appliquée uniquement aux données de `fabricpool-bucket` la . cet exemple de règle crée des copies avec code d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	2 + 1 code d'effacement pour données FabricPool
Nom du compartiment	<code>fabricpool-bucket</code> Vous pouvez également filtrer le compte de tenant FabricPool.
Filtres avancés	Taille de l'objet supérieure à 0.2 Mo. Remarque : FabricPool écrit uniquement des objets de 4 Mo, mais vous devez ajouter un filtre de taille d'objet car cette règle utilise le code d'effacement.
Heure de référence	Temps d'ingestion

Définition de règle	Exemple de valeur
Période de temps et placements	Magasin du jour 0 pour toujours Stockez les objets par code d'effacement à l'aide d'un schéma EC 2+1 à Denver et conservez-les indéfiniment dans StorageGRID.  Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool.
Comportement d'ingestion	Équilibré

2. Créez une règle ILM par défaut qui crée deux copies répliquées de tout objet non associé à la première règle. Ne sélectionnez pas de filtre de base (compte de locataire ou nom de compartiment) ni de filtre avancé.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Nom du compartiment	<i>aucun</i>
Filtres avancés	<i>aucun</i>
Heure de référence	Temps d'ingestion
Période de temps et placements	Magasin du jour 0 pour toujours Stockage d'objets en répliquant 2 copies à Denver.
Comportement d'ingestion	Équilibré

3. Créez une règle ILM et sélectionnez les deux règles. Comme la règle de réplication n'utilise aucun filtre, elle peut être la règle par défaut (dernière) de la règle.
4. Ingestion des objets de test dans la grille.
5. Simuler la règle avec les objets de test pour vérifier le comportement.
6. Activer la règle.

Lorsque cette règle est activée, StorageGRID place les données d'objet comme suit :

- Les données hiérarchisées depuis FabricPool dans `fabricpool-bucket` sont codées avec le code d'effacement 2+1. Deux fragments de données et un fragment de parité seront placés sur trois nœuds de stockage différents.
- Tous les objets dans tous les autres compartiments sont répliqués. Deux copies sont créées et placées sur deux nœuds de stockage différents.
- Les copies seront conservées dans StorageGRID indéfiniment. La solution ILM de StorageGRID ne supprime pas ces objets.

Créez une politique de classification du trafic pour FabricPool dans StorageGRID

Vous pouvez éventuellement concevoir une règle de classification du trafic StorageGRID afin d'optimiser la qualité de service pour la charge de travail FabricPool.

Pour plus de détails sur cette tâche, reportez-vous ["Gérer les stratégies de classification du trafic"](#) à la section . Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à ["Accédez à l'assistant d'installation FabricPool et terminez-le"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Description de la tâche

Les meilleures pratiques de création d'une stratégie de classification du trafic pour FabricPool dépendent de la charge de travail :

- Si vous prévoyez de transférer les données de la charge de travail principale FabricPool vers StorageGRID, vous devez vous assurer que la charge de travail FabricPool dispose de la plus grande partie de la bande passante. Vous pouvez créer une règle de classification du trafic pour limiter tous les autres workloads.



En général, les opérations de lecture FabricPool sont plus importantes que les opérations d'écriture.

Par exemple, si d'autres clients S3 utilisent ce système StorageGRID, vous devez créer une règle de classification du trafic. Vous pouvez limiter le trafic réseau pour les autres compartiments, locataires, sous-réseaux IP ou terminaux d'équilibrage de charge.

- En règle générale, vous ne devez pas imposer de limites de qualité de service à une charge de travail FabricPool, mais vous devez uniquement limiter les autres charges de travail.
- Les limites placées sur d'autres charges de travail doivent tenir compte du comportement de ces dernières. Les limites imposées varient également en fonction du dimensionnement et des capacités de votre réseau et du taux d'utilisation attendu.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.
2. Sélectionnez **Créer**.
3. Entrez un nom et une description (facultatif) pour la stratégie et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez au moins une règle.
 - a. Sélectionnez **Ajouter une règle**
 - b. Sous Type, sélectionnez **noeud final de l'équilibreur de charge**, puis sélectionnez le noeud final de l'équilibreur de charge que vous avez créé pour FabricPool.

Vous pouvez également sélectionner le compartiment ou le compte de locataire FabricPool.

- c. Si vous souhaitez que cette stratégie de trafic limite le trafic pour les autres noeuds finaux, sélectionnez **comparaison inverse**.
5. Vous pouvez également ajouter une ou plusieurs limites pour contrôler le trafic réseau correspondant à la règle.



StorageGRID collecte des mesures, même si vous n'ajoutez aucune limite, pour vous permettre de comprendre les tendances du trafic.

- a. Sélectionnez **Ajouter une limite**.
 - b. Sélectionnez le type de trafic que vous souhaitez limiter et la limite à appliquer.
6. Sélectionnez **Continuer**.
7. Lisez et passez en revue la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la stratégie, sélectionnez **Enregistrer et continuer**.

Une fois que vous avez terminé

["Afficher les données de trafic réseau"](#) pour vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Configurez ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud FabricPool

Une fois que vous avez obtenu les informations StorageGRID requises, vous pouvez accéder à ONTAP pour ajouter StorageGRID en tant que Tier cloud.

Avant de commencer

- Si vous avez terminé l'assistant d'installation de FabricPool, vous avez le fichier que vous avez `ONTAP_FabricPool_settings_bucketname.txt` téléchargé.
- Si vous avez configuré StorageGRID manuellement, vous disposez du nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou de l'adresse IP virtuelle (VIP) pour le groupe haute disponibilité StorageGRID, du numéro de port du point final de l'équilibreur de charge, du certificat d'équilibrage de charge, L'ID de clé d'accès et la clé secrète de l'utilisateur root du compte de locataire, ainsi que le nom du compartiment ONTAP seront utilisés dans ce locataire.

Accédez à ONTAP System Manager

Ces instructions expliquent comment utiliser ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud. Vous pouvez effectuer la même configuration via l'interface de ligne de commandes de ONTAP. Pour obtenir des instructions, rendez-vous sur ["Documentation ONTAP pour FabricPool"](#).

Étapes

1. Accédez à System Manager pour le cluster ONTAP que vous souhaitez mettre au niveau vers StorageGRID.
2. Connectez-vous en tant qu'administrateur du cluster.
3. Naviguez jusqu'à **STORAGE > tiers > Add Cloud Tier**.
4. Sélectionnez **StorageGRID** dans la liste des fournisseurs de magasins d'objets.

Entrez les valeurs StorageGRID

Voir ["Documentation ONTAP pour FabricPool"](#) pour plus d'informations.

Étapes

1. Remplissez le formulaire Add Cloud Tier en utilisant le `ONTAP_FabricPool_settings_bucketname.txt` fichier ou les valeurs obtenues manuellement.

Champ	Description
Nom	Entrez un nom unique pour ce niveau de cloud. Vous pouvez accepter la valeur par défaut.
Style d'URL	Si vous "Noms de domaine de terminaux S3 configurés", sélectionnez URL de type hébergement virtuel. Path-Style URL est le format par défaut pour ONTAP, mais l'utilisation de requêtes de type virtual-hosted-style est recommandée pour StorageGRID. Vous devez utiliser Path-Style URL si vous indiquez une adresse IP au lieu d'un nom de domaine dans le champ Server name (FQDN).
Nom du serveur (FQDN)	Entrez le nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou l'adresse IP virtuelle (VIP) du groupe StorageGRID HA. Par exemple <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 noeud final de l'équilibreur de charge StorageGRID. • Si vous fournissez un nom de domaine, l'enregistrement DNS doit correspondre à chaque adresse IP que vous utiliserez pour vous connecter à StorageGRID. Voir "Configurer le serveur DNS".
SSL	Activé (par défaut).
Certificat de magasin d'objets	Collez le certificat PEM que vous utilisez pour le noeud final de l'équilibreur de charge StorageGRID, notamment : -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----. Remarque : si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.
Port	Indiquez le port utilisé par le noeud final de l'équilibreur de charge StorageGRID. ONTAP utilise ce port lorsqu'il se connecte à StorageGRID. Par exemple, 10433.
Clé d'accès et clé secrète	Entrez l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root du compte de locataire StorageGRID. Conseil : si vous générez une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID à l'avenir, entrez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Sinon, ONTAP risque de perdre temporairement son accès à StorageGRID.

Champ	Description
Nom du conteneur	Indiquez le nom du compartiment StorageGRID que vous avez créé pour être utilisé avec ce niveau ONTAP.

2. Terminez la configuration finale de FabricPool dans ONTAP.
 - a. Reliez un ou plusieurs agrégats au Tier cloud.
 - b. Si vous le souhaitez, créez une règle de Tiering de volume.

Configurer les entrées du serveur DNS pour StorageGRID avec FabricPool

Après avoir configuré des groupes haute disponibilité, des terminaux d'équilibrage de la charge et des noms de domaine de terminaux S3, vous devez vous assurer que le DNS inclut les entrées nécessaires à StorageGRID. Vous devez inclure une entrée DNS pour chaque nom du certificat de sécurité et pour chaque adresse IP que vous pourriez utiliser.

Voir ["Considérations relatives à l'équilibrage de charge"](#).

Entrées DNS pour le nom du serveur StorageGRID

Ajoutez des entrées DNS pour associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez. Les adresses IP que vous entrez dans le DNS dépendent de l'utilisation ou non d'un groupe haute disponibilité de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe haute disponibilité, ONTAP se connecte aux adresses IP virtuelles de ce groupe haute disponibilité.
- Si vous n'utilisez pas de groupe haute disponibilité, ONTAP peut se connecter au service StorageGRID Load Balancer en utilisant l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.
- Si le nom du serveur résout plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP (jusqu'à 16 adresses IP). Les adresses IP sont récupérées dans une méthode de séquence périodique lors de l'établissement des connexions.

Entrées DNS pour les requêtes de type hébergement virtuel

Si vous avez défini ["Noms de domaine de terminaux S3"](#) et que vous utiliserez des requêtes de type hébergement virtuel, ajoutez des entrées DNS pour tous les noms de domaine de point de terminaison S3 requis, y compris les noms génériques.

Meilleures pratiques StorageGRID pour FabricPool

Meilleures pratiques pour les groupes de haute disponibilité (HA) StorageGRID avec FabricPool

Avant de connecter StorageGRID en tant que Tier cloud FabricPool, découvrez les groupes haute disponibilité StorageGRID et consultez les bonnes pratiques d'utilisation des groupes haute disponibilité avec FabricPool.

Qu'est-ce qu'un groupe haute disponibilité ?

Un groupe haute disponibilité est un ensemble d'interfaces issues de plusieurs nœuds de passerelle StorageGRID, nœuds d'administration ou les deux. Un groupe haute disponibilité contribue à maintenir les connexions de données des clients disponibles. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool.

Chaque groupe haute disponibilité fournit un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe haute disponibilité qui se compose d'interfaces uniquement sur les nœuds de passerelle ou sur les deux nœuds d'administration et de passerelle fournit un accès hautement disponible au service Load Balancer partagé.

Pour en savoir plus sur les groupes haute disponibilité, consultez ["Gestion des groupes haute disponibilité"](#).

À l'aide de groupes haute disponibilité

Les bonnes pratiques de création de groupe haute disponibilité StorageGRID pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec les données des principaux workloads, vous devez créer un groupe haute disponibilité incluant au moins deux nœuds d'équilibrage de la charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la règle de Tiering de volume FabricPool snapshot uniquement ou des tiers de performance locaux non principaux (par exemple, emplacements de reprise après incident ou destinations NetApp SnapMirror®), vous pouvez configurer un groupe haute disponibilité avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe haute disponibilité pour Active-Backup HA (un nœud est actif et un nœud est une sauvegarde). Cependant, vous préférez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour en savoir plus sur les avantages de ces autres configurations haute disponibilité, reportez-vous ["Options de configuration pour les groupes haute disponibilité"](#) à la section .

Meilleures pratiques pour l'équilibrage de charge StorageGRID avec FabricPool

Avant de rattacher StorageGRID en tant que Tier cloud FabricPool, consultez les bonnes pratiques pour l'utilisation d'équilibreurs de charge avec FabricPool.

Pour plus d'informations générales sur l'équilibreur de charge StorageGRID et le certificat d'équilibreur de charge, reportez-vous à la section ["Considérations relatives à l'équilibrage de charge"](#).

Bonnes pratiques pour l'accès du locataire au terminal d'équilibrage de la charge utilisé pour FabricPool

Vous pouvez contrôler les locataires qui peuvent utiliser un terminal d'équilibrage de la charge spécifique pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires, autoriser certains locataires ou bloquer certains locataires. Lors de la création d'un nœud final d'équilibrage de charge pour l'utilisation de FabricPool, sélectionnez **Autoriser tous les locataires**. ONTAP chiffre les données qui sont placées dans des compartiments StorageGRID. Cette couche de sécurité supplémentaire ne fournit donc que peu de sécurité supplémentaire.

Meilleures pratiques pour le certificat de sécurité

Lorsque vous créez un terminal d'équilibrage de charge StorageGRID pour une utilisation avec FabricPool, vous fournissez le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Dans la plupart des cas, la connexion entre ONTAP et StorageGRID doit utiliser le chiffrement TLS (transport

Layer Security). L'utilisation de FabricPool sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée. Lorsque vous sélectionnez le protocole réseau pour le noeud final de l'équilibreur de charge StorageGRID, sélectionnez **HTTPS**. Fournissez ensuite le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Pour en savoir plus sur le certificat de serveur pour un point final d'équilibrage de charge :

- ["Gérer les certificats de sécurité"](#)
- ["Considérations relatives à l'équilibrage de charge"](#)
- ["Consignes de renforcement des certificats de serveur"](#)

Ajouter le certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau de cloud FabricPool, vous devez installer le même certificat sur le cluster ONTAP, y compris le certificat racine et tout certificat d'autorité de certification subordonnée.

Gérer l'expiration des certificats



Si le certificat utilisé pour sécuriser la connexion entre ONTAP et StorageGRID expire, FabricPool cesse temporairement de fonctionner et ONTAP perd temporairement l'accès aux données hiérarchisées vers StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez les bonnes pratiques suivantes :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que le **expiration du certificat de noeud final de l'équilibreur de charge** et le **expiration du certificat de serveur global pour les alertes de l'API S3**.
- Gardez toujours les versions StorageGRID et ONTAP du certificat synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le Tier cloud.
- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez utiliser l'API de gestion de grille pour automatiser la rotation des certificats. Vous pouvez ainsi remplacer les certificats dont la date d'expiration arrive à expiration sans interrompre l'activité.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans ONTAP avant que le certificat existant n'expire. Si un certificat auto-signé a déjà expiré, désactivez la validation du certificat dans ONTAP pour éviter toute perte d'accès.

Voir ["Base de connaissances NetApp : comment configurer un nouveau certificat de serveur autosigné StorageGRID sur un déploiement ONTAP FabricPool existant"](#) pour obtenir des instructions.

Meilleures pratiques pour l'utilisation de StorageGRID ILM avec les données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez connaître les exigences d'utilisation de la gestion du cycle de vie des informations (ILM) StorageGRID avec les données FabricPool.



FabricPool ne connaît pas les règles ou les règles ILM de StorageGRID. La perte des données peut se produire si la règle ILM de StorageGRID est mal configurée. Pour plus d'informations, voir ["Les règles ILM permettent de gérer les objets"](#) et ["Création de règles ILM"](#).

Règles d'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant d'installation FabricPool, il crée automatiquement une règle ILM pour chaque compartiment S3 que vous créez, puis l'ajoute à une règle inactive. Vous êtes invité à activer la stratégie. La règle automatiquement créée respecte les bonnes pratiques recommandées : elle utilise un code d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant d'installation FabricPool, lisez ces instructions pour vous assurer que les règles ILM et la politique ILM sont adaptées aux données FabricPool et aux exigences de votre entreprise. Vous devrez peut-être créer de nouvelles règles et mettre à jour vos règles ILM actives pour répondre à ces instructions.

- Vous pouvez utiliser toutes les combinaisons de réplication et de règles de code d'effacement pour protéger les données de Tier cloud.

Il est recommandé d'utiliser un code d'effacement 2+1 sur un site pour une protection des données économique. Le code d'effacement consomme plus de ressources de processeur, mais sa capacité de stockage est bien inférieure à la réplication. Les schémas 4+1 et 6+1 utilisent moins de capacité que le schéma 2+1. Toutefois, les schémas 4+1 et 6+1 sont moins flexibles si vous avez besoin d'ajouter des nœuds de stockage lors de l'extension de grid. Pour plus de détails, voir ["Ajoutez de la capacité de stockage pour les objets avec code d'effacement"](#).

- Chaque règle appliquée aux données FabricPool doit au moins deux copies répliquées grâce au code d'effacement.



La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

- Si vous avez besoin de ["Supprimez les données FabricPool de StorageGRID"](#), utilisez ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir auprès du Tier de performance.



Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation de chaque règle ILM sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

- Ne créez pas de règles qui déplacera les données de Tier cloud FabricPool hors du compartiment vers un autre emplacement. Vous ne pouvez pas utiliser un pool de stockage cloud pour déplacer des données FabricPool vers un autre magasin d'objets.



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

- Depuis ONTAP 9.8, vous pouvez créer des balises d'objet pour classer et trier les données hiérarchisées pour simplifier la gestion. Par exemple, vous pouvez définir des balises uniquement sur les volumes FabricPool reliés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous

pouvez utiliser le filtre avancé balise d'objet pour sélectionner et placer ces données.

Meilleures pratiques pour les paramètres globaux de StorageGRID avec FabricPool

Lors de la configuration d'un système StorageGRID pour une utilisation avec FabricPool, vous devrez peut-être modifier d'autres options StorageGRID. Avant de modifier un paramètre global, réfléchissez à l'impact de cette modification sur les autres applications S3.

Vérifiez les destinations des messages et des journaux

Les charges de travail FabricPool disposent souvent d'un taux élevé d'opérations de lecture, ce qui peut générer un grand nombre de messages d'audit.

- Si vous n'avez pas besoin d'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 la gestion des journaux et le serveur syslog externe](#)" 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 réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir "[Considérations relatives au serveur syslog externe](#)" pour plus de détails.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le "[option globale de chiffrement des objets stockés](#)" si le chiffrement des données est requis pour d'autres clients StorageGRID. Les données envoyées depuis FabricPool vers StorageGRID sont déjà chiffrées, ce qui signifie qu'il n'est pas nécessaire d'activer le paramètre StorageGRID. Les clés de chiffrement côté client sont la propriété de ONTAP.

Compression d'objet

Lors de la configuration de StorageGRID, n'activez pas "[option globale pour compresser les objets stockés](#)". Les données envoyées depuis FabricPool vers StorageGRID sont déjà compressées. L'utilisation de l'option StorageGRID ne réduira pas davantage la taille d'un objet.

Verrouillage d'objet S3

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, ne l'activez pas "[Verrouillage d'objet S3](#)" lorsque vous créez des buckets FabricPool. Le verrouillage d'objet S3 n'est pas pris en charge pour les buckets FabricPool.

Cohérence du compartiment

Pour les compartiments FabricPool, la cohérence de compartiment recommandée est **Read-After-New-write**, ce qui correspond à la cohérence par défaut d'un nouveau compartiment. Ne modifiez pas les compartiments FabricPool pour utiliser **disponible** ou **site fort**.

Hiérarchisation FabricPool

Si un nœud StorageGRID utilise du stockage attribué à un système NetApp ONTAP, vérifiez qu'aucune règle de hiérarchisation FabricPool n'est activée sur le volume. Par exemple, si un nœud StorageGRID s'exécute

sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n'est pas activée sur le volume qui sauvegarde le datastore pour le nœud StorageGRID. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Supprimez les données FabricPool de StorageGRID

Si vous devez supprimer les données FabricPool qui sont actuellement stockées dans StorageGRID, vous devez utiliser ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir dans le Tier de performance.

Avant de commencer

- Vous avez examiné les instructions et les considérations de la section ["Promouvoir les données vers le Tier de performance"](#).
- Vous utilisez ONTAP 9.8 ou une version ultérieure.
- Vous utilisez un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs StorageGRID pour le compte de tenant FabricPool qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#).

Description de la tâche

Ces instructions expliquent comment transférer des données de StorageGRID vers FabricPool. Cette procédure s'effectue à l'aide de ONTAP et du Gestionnaire de locataires StorageGRID.

Étapes

1. Depuis ONTAP, exécutez la `volume modify` commande.

Définissez `tiering-policy` sur `none` pour arrêter le nouveau Tiering et définissez `cloud-retrieval-policy` sur `promote` pour renvoyer toutes les données qui ont été auparavant hiérarchisées vers StorageGRID.

Voir ["Promotion de toutes les données d'un volume FabricPool vers le Tier de performance"](#).

2. Attendez la fin de l'opération.

Vous pouvez utiliser `volume object-store` la commande avec `tiering` l'option pour ["vérifier le statut de la promotion du niveau de performances"](#).

3. Une fois l'opération de promotion terminée, connectez-vous au gestionnaire de locataires StorageGRID pour le compte de locataire FabricPool.
4. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
5. Vérifiez que le compartiment FabricPool est vide.
6. Si le godet est vide, ["supprimez le compartiment"](#).

Une fois que vous avez terminé

Lorsque vous supprimez le compartiment, le Tiering de FabricPool vers StorageGRID ne peut plus se poursuivre. Cependant, le niveau local étant toujours attaché au niveau cloud StorageGRID, ONTAP System Manager renvoie des messages d'erreur indiquant que le compartiment est inaccessible.

Pour éviter ces messages d'erreur, effectuez l'une des opérations suivantes :

- Utilisez FabricPool Mirror pour associer un Tier cloud différent à l'agrégat.
- Déplacez les données de l'agrégat FabricPool vers un agrégat non FabricPool, puis supprimez l'agrégat non utilisé.

Reportez-vous ["Documentation ONTAP pour FabricPool"](#) au pour obtenir des instructions.

Utilisez les locataires et clients StorageGRID

Utilisez un compte de locataire

Utilisez un compte de locataire StorageGRID

Un compte de locataire vous permet d'utiliser l'API REST simple Storage Service (S3) pour stocker et récupérer des objets dans un système StorageGRID.

Qu'est-ce qu'un compte de locataire ?

Chaque compte de locataire dispose de ses propres groupes, utilisateurs, compartiments S3 et objets fédérés ou locaux.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Utilisation en entreprise** : si le système StorageGRID est utilisé au sein d'une entreprise, le stockage objet de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes de tenant pour le service Marketing, le service Customer support, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez également utiliser des 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 "[Compartiments S3 et règles de compartiments](#)" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services** : si le système StorageGRID est utilisé par un fournisseur de services, le stockage objet de la grille peut être séparé par les différentes entités qui louent le stockage. Il peut s'agir, par exemple, de comptes de locataires pour la société A, la société B, la société C, etc.

Comment créer un compte de locataire

Les comptes de tenant sont créés par un "[Administrateur du grid StorageGRID utilisant le gestionnaire de grille](#)". Lors de la création d'un compte de locataire, l'administrateur de la grille spécifie ce qui suit :

- Informations de base comprenant le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, les administrateurs du grid peuvent activer le paramètre de verrouillage objet S3 pour le système StorageGRID si les comptes de locataires S3 doivent être conformes aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

Configurez les locataires S3

Après un ["Le compte de locataire S3 est créé"](#), vous pouvez accéder au gestionnaire de locataires pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération de grilles pour la synchronisation des comptes et la réplication inter-grilles
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage



Bien que vous puissiez créer et gérer des compartiments S3 avec le gestionnaire des locataires, vous devez utiliser un ["Client S3"](#) ou ["Console S3"](#) pour ingérer et gérer les objets.

Comment se connecter et se déconnecter

Se connecter à StorageGRID Tenant Manager

Vous accédez au gestionnaire de locataires en entrant l'URL du locataire dans la barre d'adresse d'un ["navigateur web pris en charge"](#).

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL permettant d'accéder au gestionnaire de locataires, fournie par votre administrateur de grille. L'URL se présente comme l'un de ces exemples :

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL inclut toujours un nom de domaine complet (FQDN), l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous disposez de cet ID de compte.
- Vous utilisez un ["navigateur web pris en charge"](#).
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs qui a ["autorisations d'accès spécifiques"](#).

Étapes

1. Lancez un ["navigateur web pris en charge"](#).

2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire de locataires.

L'écran d'ouverture de session qui s'affiche dépend de l'URL que vous avez saisie et de la configuration de l'authentification unique (SSO) pour StorageGRID.

Pas d'utilisation de SSO

Si StorageGRID n'utilise pas SSO, l'un des écrans suivants s'affiche :

- Page de connexion de Grid Manager. Sélectionnez le lien **tenant sign-in**.
- La page de connexion du gestionnaire de locataires. Le champ **Compte** est peut-être déjà rempli.
 - i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.
 - ii. Saisissez votre nom d'utilisateur et votre mot de passe.
 - iii. Sélectionnez **connexion**.

Le tableau de bord du gestionnaire de locataires s'affiche.

- iv. Si vous avez reçu un mot de passe initial de la part d'une autre personne, sélectionnez **username > change password** pour sécuriser votre compte.

Utilisation de SSO

Si StorageGRID utilise SSO, l'un des écrans suivants s'affiche :

- La page SSO de votre organisation.

Entrez vos informations d'identification SSO standard et sélectionnez **se connecter**.

- Page de connexion SSO du Gestionnaire de locataires.
 - i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.
 - ii. Sélectionnez **connexion**.
 - iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord du gestionnaire de locataires s'affiche.

Déconnexion de StorageGRID Tenant Manager

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Localisez la liste déroulante Nom d'utilisateur dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez le nom d'utilisateur, puis sélectionnez **Déconnexion**.

- Si SSO n'est pas utilisé :

Vous êtes déconnecté du nœud d'administration. La page de connexion au Gestionnaire de locataires s'affiche.



Si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.

- Si SSO est activé :

Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche.



Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Tableau de bord Tenant Manager dans StorageGRID

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 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.



La taille logique de tous les objets appartenant à ce locataire inclut les téléchargements multipartites incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. 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 :

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

Informations sur le compte locataire

Le haut du tableau de bord affiche le nombre de compartiments ou de conteneurs, de groupes et d'utilisateurs configurés. Il affiche également le nombre de noeuds finaux de services de plate-forme, s'ils ont été configurés. Sélectionnez les liens pour afficher les détails.

Selon votre configuration et les options dont vous disposez, le reste du tableau de bord affiche différentes combinaisons de consignes, d'utilisation du stockage, d'informations sur l'objet et de données sur le "autorisations de gestion des locataires" locataire.

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

- Si un quota est défini, la quantité totale d'espace disponible pour les données d'objet ainsi que la quantité et le pourcentage d'espace restant. Le quota limite la quantité de données d'objet pouvant être ingérées.



L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.

- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs.

Vous pouvez placer le curseur sur n'importe quel segment de graphique pour afficher l'espace total utilisé par ce compartiment ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands seaux ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque godet ou conteneur.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

Si le locataire possède plus de neuf compartiments ou conteneurs, tous les autres compartiments ou conteneurs sont regroupés en une seule entrée au bas de la liste.



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de locataires, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de locataires, puis sélectionnez **Préférences utilisateur**.

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, ces alertes apparaissent dans le gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

- Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **usage du quota de locataire élevé** est déclenchée.

Demandez à votre administrateur de grid d'augmenter le quota.

- Si vous dépassez votre quota, une notification vous indique que vous ne pouvez pas télécharger de nouveaux objets.

utilisation limitée de la capacité

Si vous avez défini une limite de capacité pour vos compartiments, le tableau de bord du gestionnaire de locataires affiche la liste des principaux compartiments par utilisation de la limite de capacité.

Si aucune limite n'est définie pour un godet, sa capacité est illimitée. Toutefois, 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 pour un compartiment.

Erreurs de point final

Si vous avez utilisé le gestionnaire de grille pour configurer un ou plusieurs points de terminaison pour les services de plateforme, le tableau de bord du gestionnaire de locataires affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.



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 "[erreurs de noeud final des services de plate-forme](#)" afficher des détails sur , sélectionnez **noeuds finaux** pour afficher la page noeuds finaux.

API de gestion des locataires

Découvrez l'API de gestion des locataires StorageGRID

Vous pouvez effectuer des tâches de gestion du système via l'API REST de gestion des locataires plutôt que dans l'interface utilisateur du gestionnaire de locataires. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API de gestion des locataires :

- Utilise la plate-forme API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.
- Utilise "[gestion des versions pour prendre en charge les mises à niveau sans interruption](#)".

Pour accéder à la documentation de swagger pour l'API de gestion des locataires :

1. Connectez-vous au Gestionnaire de locataires.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.

Opérations API

L'API de gestion des locataires organise les opérations API disponibles dans les sections suivantes :

- **Compte** : opérations sur le compte locataire actuel, y compris l'obtention d'informations sur l'utilisation du stockage.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour une connexion locataire, vous devez fournir un nom d'utilisateur, un mot de passe et un ID de compte dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : jeton porteur »).

Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section ["Protéger contre la contrefaçon de demandes intersites"](#).



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir la ["Instructions d'utilisation de l'API de gestion de grille"](#).

- **Config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **conteneurs** : opérations sur les buckets S3.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **Noeuds finaux** : opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication de grille transversale.
- **Groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **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.
- **configurations s3** : opérations permettant de récupérer les configurations globales S3.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **Utilisateurs** : opérations pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

Lorsque vous développez chaque opération d'API, vous pouvez voir son action HTTP, son URL de point final, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.

groups

Operations on groups

GET

/org/groups

Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order 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": "2.0" }</pre>

Émettre des requêtes API



Toutes les opérations d'API que vous effectuez à l'aide de la page Web Documentation de l'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 afficher les détails de la demande.
2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.

4. Sélectionnez **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Sélectionnez **Exécuter**.
7. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Versionnage de l'API de gestion des locataires StorageGRID

L'API de gestion des locataires utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La version majeure de l'API est incrémentée lorsque des modifications sont effectuées qui ne sont *pas compatibles* avec des versions plus anciennes. La version mineure de l'API est incrémentée lorsque des modifications qui sont *compatibles* avec des versions plus anciennes sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2,1	2,2
Non compatible avec les versions plus anciennes	2,1	3,0

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 StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.



Vous pouvez configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section **config** de la documentation de l'API swagger "[API de gestion du grid](#)". Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la nouvelle version.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la GET `/versions` requête API pour renvoyer une liste des versions majeures de l'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
  ]
}
```

Spécifiez une version API pour une demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (`/api/v4`) ou d'un en-tête (`Api-Version: 4`). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protégez-vous contre la falsification de requêtes intersites (CSRF) dans StorageGRID

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez le `csrfToken` paramètre sur `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Lorsque la valeur est true, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- L'`X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé en forme : un `csrfToken` paramètre de corps de requête codé en forme.

Pour configurer la protection CSRF, utilisez le ou le ["API de gestion du grid"](#) ["API de gestion des locataires"](#).



Les demandes qui ont un ensemble de cookies de token CSRF appliquent également l'en-tête « Content-Type: Application/json » pour toute demande qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de fédération de grille

Synchronisez les groupes de locataires et les utilisateurs dans StorageGRID

Si un locataire a été créé ou modifié pour utiliser des connexions de fédération de grilles, ce locataire est répliqué d'un système StorageGRID (le locataire source) vers tous les autres systèmes StorageGRID connectés (les locataires répliqués). Après la réplication du locataire, les groupes de locataires, les utilisateurs et les clés d'accès S3 sont synchronisés entre les grilles connectées.

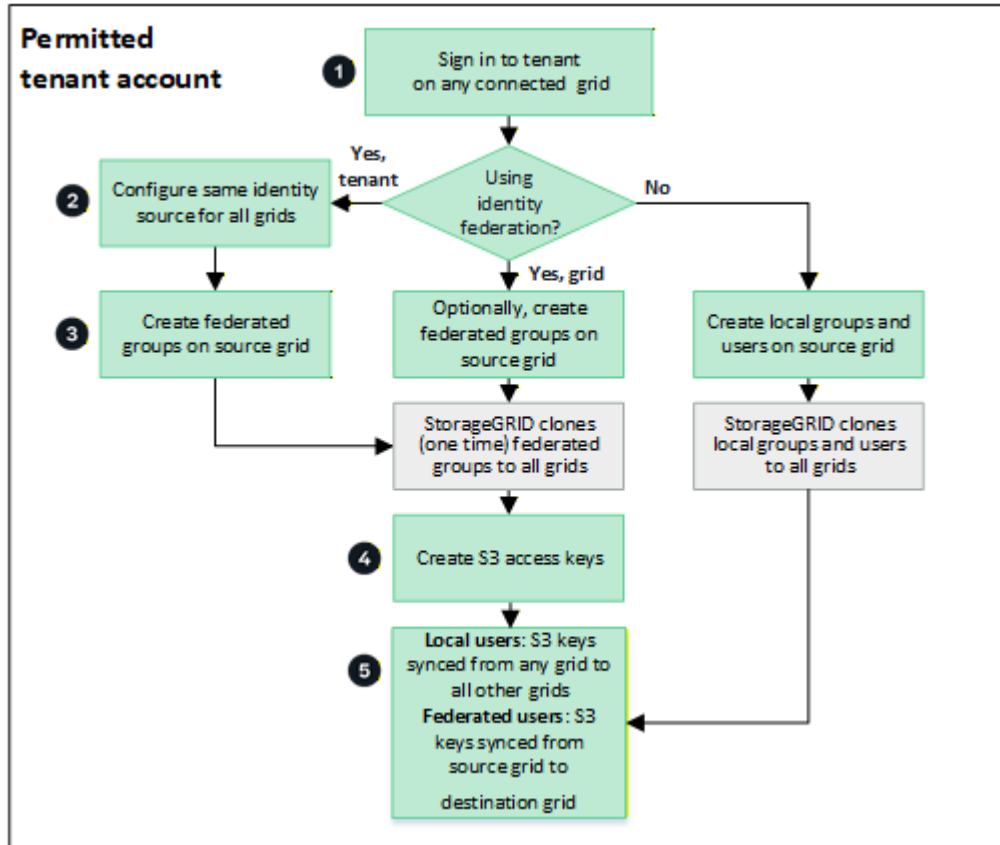
Le système StorageGRID dans lequel le locataire est initialement créé est la *grille source* du locataire. Le locataire est répliqué sur une ou plusieurs *grilles de destination*. Les comptes locataires sur toutes les grilles connectées possèdent les mêmes ID de compte, nom, description, quota de stockage, autorisations attribuées et mot de passe de l'utilisateur root. Pour plus de détails, reportez-vous à ["Découvrez la synchronisation des comptes pour la fédération de grilles"](#) et ["Gérer les locataires autorisés"](#).

La synchronisation des informations des comptes locataires est nécessaire pour ["réplication entre plusieurs grilles"](#) des objets de compartiment. Avoir les mêmes groupes de locataires et les mêmes utilisateurs sur toutes les grilles garantit que vous pouvez accéder aux compartiments et objets correspondants sur n'importe quelle grille connectée.

Flux de travail du locataire pour la synchronisation des comptes

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, consultez le

diagramme de flux de travail pour voir les étapes que vous effectuerez pour synchroniser les groupes, les utilisateurs et les clés d'accès S3.



Voici les principales étapes du flux de travail :

1

Connectez-vous au locataire

Connectez-vous au compte locataire sur n'importe quelle grille connectée.

2

Vous pouvez également configurer la fédération des identités

Si votre compte locataire dispose de l'autorisation **Utiliser sa propre source d'identité** pour utiliser les groupes et utilisateurs fédérés, configurez la même source d'identité (avec les mêmes paramètres) pour le compte source et un ou plusieurs comptes locataires de destination. Les groupes fédérés sont clonés lors de leur création et les utilisateurs fédérés sont clonés lors de la création d'une clé. Pour que le clonage ait lieu, la même source d'identité doit être configurée sur toutes les grilles. Pour obtenir des instructions, consultez ["Utiliser la fédération des identités"](#).

3

Créer des groupes et des utilisateurs

Vous pouvez créer des groupes et des utilisateurs depuis n'importe quelle grille connectée. Lorsque vous ajoutez un nouveau groupe local, StorageGRID le synchronise automatiquement avec toutes les grilles connectées. Les modifications des groupes locaux (modification, suppression) sont également synchronisées en continu. Les groupes fédérés sont clonés une seule fois lors de leur création.

- Si la fédération des identités est configurée pour l'ensemble du système StorageGRID ou pour votre

compte de locataire, "[créer de nouveaux groupes de locataires](#)" en important des groupes fédérés à partir du référentiel d'identité.

- Si vous n'utilisez pas la fédération d'identité, "[créer de nouveaux groupes locaux](#)" et puis "[créer des utilisateurs locaux](#)".

4

Création de clés d'accès S3

Vous pouvez "[créer vos propres clés d'accès](#)" ou "[créer les clés d'accès d'un autre utilisateur](#)" sur n'importe quelle grille pour accéder aux compartiments sur toutes les grilles connectées.

5

Synchroniser les clés d'accès S3

Si vous devez accéder à des compartiments avec les mêmes clés d'accès sur toutes les grilles, créez les clés d'accès sur l'une des grilles. Pour les utilisateurs locaux, les clés d'accès sont synchronisées automatiquement par défaut. Pour les utilisateurs fédérés, vous devez créer les clés d'accès S3 sur la grille source et sélectionner **Activer la synchronisation des clés d'accès** pour que les clés soient synchronisées avec toutes les grilles de destination.

Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils synchronisés ?

Consultez cette section pour comprendre comment les groupes, les utilisateurs et les clés d'accès S3 sont synchronisés entre les grilles connectées.

Les groupes locaux sont synchronisés en permanence

Une fois le compte locataire créé et répliqué sur la grille de destination, StorageGRID synchronise en continu les groupes locaux sur toutes les grilles connectées. Toutes les modifications apportées aux groupes locaux, y compris les opérations de création, de modification et de suppression, effectuées sur une grille sont automatiquement répliquées sur toutes les autres grilles connectées.

Le groupe d'origine et ses copies synchronisées possèdent le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3. Pour obtenir des instructions, consultez "[Créez des groupes pour les locataires S3](#)".

Les utilisateurs locaux sont synchronisés en continu

Lorsque vous créez un nouvel utilisateur local sur une grille connectée, StorageGRID synchronise automatiquement cet utilisateur avec toutes les autres grilles connectées. Les modifications ultérieures, y compris les éditions, suppressions et réinitialisations de mot de passe, sont également synchronisées en continu. L'utilisateur d'origine et ses copies synchronisées possèdent le même nom complet, le même nom d'utilisateur et le même paramètre **Refuser l'accès**. Les mêmes utilisateurs sur chaque grille appartiennent également aux mêmes groupes. Pour obtenir des instructions, consultez "[Gérer les utilisateurs](#)".

Les groupes fédérés sont synchronisés une seule fois lors de leur création

Si les conditions requises pour utiliser la synchronisation des comptes avec "[authentification unique](#)" et "[fédération des identités](#)" ont été remplies, les groupes fédérés que vous créez (importez) pour le locataire sur une grille sont automatiquement synchronisés avec le locataire sur toutes les autres grilles connectées.

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 synchronisés avec les autres grilles, les utilisateurs fédérés peuvent se connecter au locataire depuis n'importe quelle grille connectée. Les modifications ultérieures apportées aux groupes fédérés ne sont pas automatiquement synchronisées entre les grilles.

Les clés d'accès S3 peuvent être synchronisées automatiquement ou manuellement

Par défaut, StorageGRID synchronise automatiquement les clés d'accès S3. Pour des raisons de sécurité, vous pouvez désactiver la synchronisation automatique des clés d'accès S3 pour chaque tenant et utiliser des clés différentes pour chaque tenant sur chaque grille.

Pour gérer les clés d'accès sur les réseaux connectés, vous pouvez procéder de l'une des manières suivantes :

- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grid, vous pouvez désactiver la synchronisation automatique des clés d'accès et "[créez vos propres clés d'accès](#)" ou "[créez les clés d'accès d'un autre utilisateur](#)" sur chaque grid.



Lorsque vous synchronisez les clés d'accès S3 pour un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont synchronisés avec les locataires de destination.



Les clés d'accès S3 appartenant aux utilisateurs locaux sont synchronisées en continu entre les grilles connectées, y compris lors de la suppression des clés. Les clés d'accès S3 appartenant aux utilisateurs fédérés sont synchronisées une seule fois lors de leur création ; les modifications ultérieures, y compris les suppressions, ne sont pas répliquées. Vous pouvez activer ou désactiver la synchronisation des clés d'accès pour chaque connexion de locataire.

Les groupes et les utilisateurs ajoutés à la grille de destination sont synchronisés

Les modifications apportées à n'importe quelle grille connectée, y compris la création ou l'importation de groupes et d'utilisateurs locaux, sont automatiquement synchronisées avec toutes les autres grilles connectées.

Les groupes locaux, les utilisateurs et les clés d'accès modifiés ou supprimés sont synchronisés

Les modifications apportées aux groupes locaux, aux utilisateurs locaux et aux clés d'accès S3 appartenant à des utilisateurs locaux sont synchronisées en continu sur toutes les grilles connectées. Les opérations synchronisées comprennent les modifications, les suppressions et les réinitialisations de mot de passe.

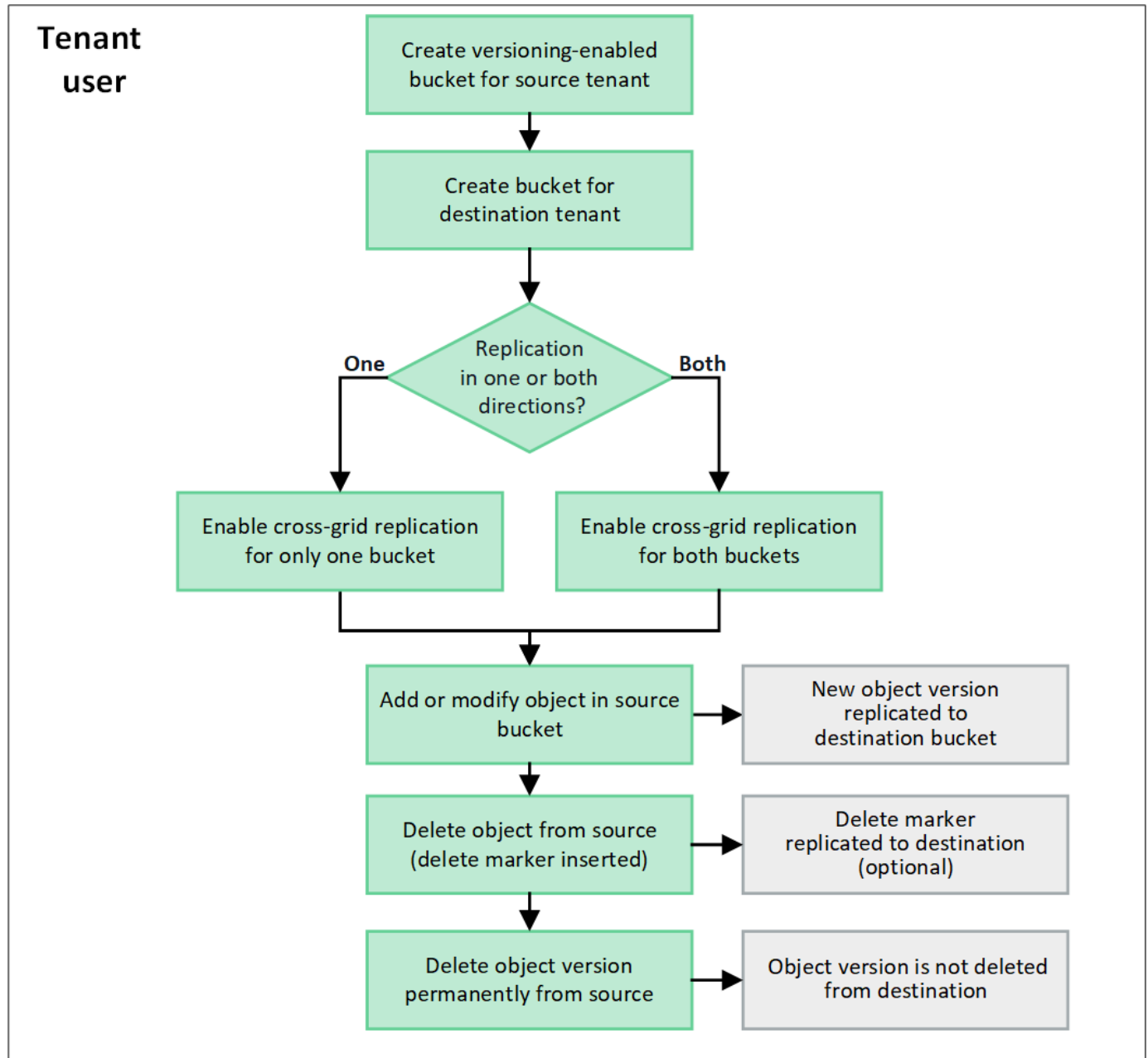
Les modifications apportées aux groupes fédérés et aux clés d'accès S3 appartenant aux utilisateurs fédérés ne sont pas synchronisées après leur création initiale.

Gérer la réplication inter-grilles dans StorageGRID

Si l'autorisation **utiliser la connexion de fédération de grille** a été attribuée à votre compte de locataire lors de sa création, vous pouvez utiliser la réplication multigrille pour répliquer automatiquement les objets entre les compartiments de la grille source du locataire et les compartiments de la grille de destination du locataire. La réplication inter-grille peut se produire dans une ou les deux directions.

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail résume les étapes à suivre pour configurer la réplication inter-grille entre les buckets de deux grilles. Ces étapes sont décrites plus en détail sous le diagramme.



Configurer la réplication entre les grilles

Avant de pouvoir utiliser la réplication inter-grille, vous devez vous connecter aux comptes locataires correspondants sur chaque grille et créer deux buckets. 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-grille. ["Qu'est-ce que la réplication cross-grid"](#) .
- 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. "[Gérez les locataires autorisés pour la connexion de fédération de grille](#)".
- L'utilisateur locataire sous lequel vous vous connectez existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".
- Si vous vous connectez à la grille de destination du locataire en tant qu'utilisateur local, l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur sur cette grille.

Créer deux buckets

Dans un premier temps, connectez-vous aux comptes locataires correspondants sur chaque grille et créez un bucket sur chaque grille.

Étapes

1. En commençant à partir de l'une des grilles de la connexion de fédération de grille, créez un nouveau compartiment :
 - a. Connectez-vous au compte de tenant à l'aide des informations d'identification d'un utilisateur de tenant qui existe sur les deux grilles.

Si vous ne parvenez pas à vous connecter à la grille de destination du locataire en tant qu'utilisateur local, confirmez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

 - b. Suivez les instructions à "[Créer un compartiment S3](#)".

Les noms des buckets et des régions peuvent être différents sur chaque grille.

 - c. Dans l'onglet **gérer les paramètres d'objet**, sélectionnez **Activer la gestion des versions d'objet**.
 - d. Si le verrouillage d'objet S3 est activé pour votre système StorageGRID , reportez-vous à "[Réplication inter-grille avec S3 Object Lock](#)".
 - e. Sélectionnez **Créer un compartiment**.
 - f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un bucket pour le même compte locataire sur l'autre grille dans la connexion de fédération de grille.



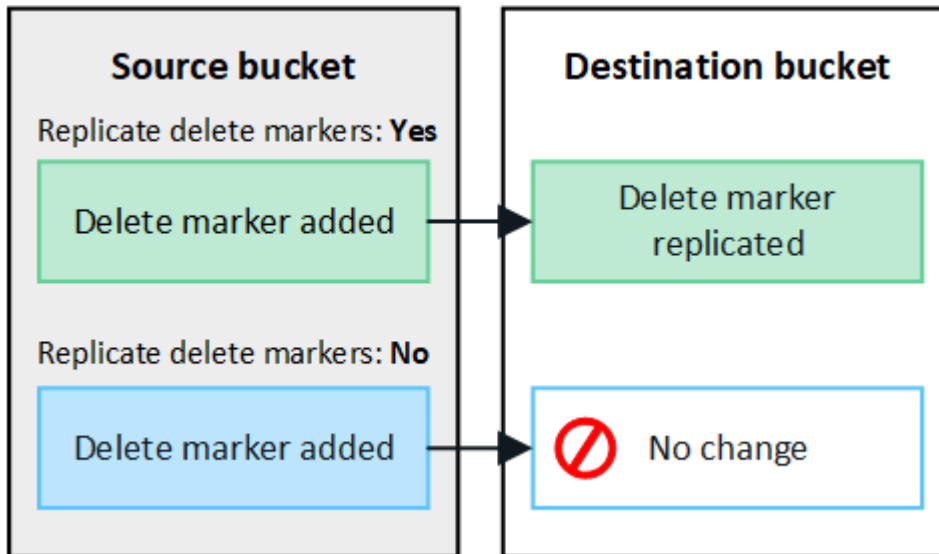
Selon les besoins, chaque godet peut utiliser une région différente.

Activer la réplication entre les grilles

Étapes

1. À partir d'une grille dont vous voulez répliquer les objets, activez "[réplication multigrille dans une direction](#)":
 - a. Connectez-vous au compte du locataire pour le compartiment.
 - b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
 - c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
 - d. Sélectionnez l'onglet **réplication multigrille**.

- e. Sélectionnez **Activer** et consultez la liste des exigences.
- f. Si toutes les exigences ont été satisfaites, sélectionnez la connexion de fédération de grille que vous souhaitez utiliser.
- g. Vous pouvez également modifier le paramètre **replicate delete markers** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une demande de suppression à la grille source qui n'inclut pas d'ID de version :
 - **Yes** (par défaut) : un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment 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.

Se référer à ["Qu'est-ce que la réplification cross-grid"](#) pour plus de détails.

- a. Vous pouvez également modifier le paramètre de la catégorie d'audit **réplication multigrille** pour gérer le volume des messages d'audit :
 - **Erreur** (par défaut) : seules les demandes de réplification inter-grille en échec sont incluses dans la sortie d'audit.
 - **Normal** : toutes les demandes de réplification inter-grille sont incluses, ce qui augmente considérablement le volume de la sortie d'audit.
- b. Sélectionnez **Activer et tester**.

Après quelques instants, un message de réussite apparaît. Les objets ajoutés à ce bucket sont 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. Si vous le souhaitez, accédez au compartiment correspondant sur l'autre grille et ["activez la réplification entre les grilles dans les deux sens"](#).

Tester la réplication entre les grilles

Si la réplication inter-grid est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réplication inter-grid fonctionnent correctement et que les compartiments source et de destination répondent toujours à toutes les exigences (par exemple, la gestion des versions est toujours activée).

Avant de commencer

- Vous utilisez un ["navigateur web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).

Étapes

1. Connectez-vous au compte du locataire pour le compartiment.
2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
4. Sélectionnez l'onglet **réplication multigrille**.
5. Sélectionnez **Tester la connexion**.

Si la connexion est 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, reportez-vous à ["Dépanner les erreurs de fédération de grille"](#) .

6. Si la réplication inter-grille est configurée pour se produire dans les deux sens, allez dans le compartiment correspondant sur l'autre grille et sélectionnez **Tester la connexion** pour vérifier que la réplication inter-grille fonctionne dans l'autre sens.

Désactiver la réplication entre les grilles

Vous pouvez arrêter définitivement la réplication multigrille si vous ne souhaitez plus copier d'objets sur l'autre grille.

Avant de désactiver la réplication multigrille, notez ce qui suit :

- La désactivation de la réplication 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-grid a été activée pour chacun des compartiments (c'est-à-dire si la réplication se produit dans les deux directions), vous pouvez désactiver la réplication inter-grid pour l'un ou les deux compartiments. Par exemple, vous pouvez désactiver la réplication d'objets de `my-bucket` sur la grille 1 vers `my-bucket` sur la grille 2, tout en continuant à répliquer des objets de `my-bucket` sur la grille 2 vers `my-bucket` 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. ["Gérer les locataires autorisés"](#) .

Avant de commencer

- Vous utilisez un ["navigateur web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).

Étapes

1. Depuis la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grid pour le compartiment :
 - a. Connectez-vous au compte du locataire pour le compartiment.
 - b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
 - c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
 - d. Sélectionnez l'onglet **réplication multigrille**.
 - e. Sélectionnez **Désactiver la réplication**.
 - f. Si vous êtes sûr de vouloir désactiver la réplication inter-grille pour ce bucket, saisissez **Oui** dans la zone de texte et sélectionnez **Désactiver**.

Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être automatiquement répliqués sur l'autre grille. **La réplication multigrille** n'est plus affichée comme fonction activée sur la page compartiments.

2. Si la réplication inter-grille a été configurée pour se produire dans les deux directions, allez dans le compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre direction.

Afficher les connexions de fédération de grilles dans StorageGRID

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez afficher les connexions autorisées.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Grid federation connections**.

La page de connexion de fédération de grille s'affiche et comprend un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de fédération de grille que ce locataire a l'autorisation d'utiliser.
Compartiments avec réplication inter-grid	Pour chaque connexion de fédération de grid, les compartiments de locataire pour lesquels la réplication inter-grid est activée. Les objets ajoutés à ces compartiments seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente se produit, le cas échéant, lors de la réplication des données vers l'autre grille. Voir Effacez la dernière erreur .

2. Si vous le souhaitez, sélectionnez un nom de compartiment à "afficher les détails du compartiment".

efface la dernière erreur

Une erreur peut apparaître dans la colonne **dernière erreur** pour l'une des raisons suivantes :

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.



Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées.

Étapes

1. Si un message apparaît dans la colonne **dernière erreur**, affichez le texte du message.

Par exemple, cette erreur indique que le compartiment de destination de la réplication inter-grid était dans un état non valide, probablement parce que la gestion de version a été suspendue ou que le verrouillage d'objet S3 a été activé.

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 la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.

3. Sélectionnez la connexion dans le tableau.

4. Sélectionnez **Effacer erreur**.

5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.

6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, reportez-vous à la section ["Identifier et réessayer les opérations de réplcation ayant échoué"](#).

Gestion des groupes et des utilisateurs

Utilisez la fédération d'identité dans StorageGRID

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

Configurez la fédération des identités pour le gestionnaire des locataires

Vous pouvez configurer la fédération 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, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).
- Vous utilisez Active Directory, Microsoft Entra ID, 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 avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Instructions de configuration du serveur OpenLDAP](#).
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir ["Chiffrement pris en charge pour les connexions TLS sortantes"](#).

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct pour ce locataire.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Entrez la configuration

Lorsque vous configurez la fédération Identify, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **Gestion des accès > Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identités**.

3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
- **Nom unique 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, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
- **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
 - **Port** : port utilisé pour se connecter au serveur LDAP.



Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- sAMAccountName ou uid
 - objectGUID, entryUUID ou nsuniqueid
 - cn
 - memberOf ou isMemberOf
 - **Active Directory** : objectSid, primaryGroupID, userAccountControl et userPrincipalName
 - **Entra ID**: accountEnabled et userPrincipalName
- **Mot de passe** : 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 de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.



Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

- **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

- **Modèle UserPrincipalName (AD et Entra ID)**: [USERNAME]@example.com
- **Modèle de nom de connexion de niveau inférieur (AD et Entra ID)**: example\[USERNAME]
- **Motif de nom distinctif** : CN=[USERNAME],CN=Users,DC=example,DC=com

Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

- **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 Microsoft Entra ID.
- **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Microsoft Entra ID.
- **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 Microsoft Entra ID.



L'utilisation de l'option **Ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
 - Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s'affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Si les paramètres de connexion ne sont pas valides, le message « Impossible d'établir la connexion de test » s'affiche. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.

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

- Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s'affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.



L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération 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.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et la source d'identité ne se produira pas 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'état de l'authentification unique (SSO) est **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 des identités.
2. Décochez la case **Activer la fédération d'identité**.

Instructions de configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les sources d'identité qui ne sont pas Active Directory ou Microsoft Entra ID, 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.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinement doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance des membres de groupe inversé dans le ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"](#).

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations sur la maintenance de l'appartenance à ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"](#) un groupe inversé dans le .

Gestion des groupes de locataires

Créez des groupes pour un locataire S3 dans StorageGRID

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des groupes fédérés ou en créant des groupes locaux.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).
- Si vous prévoyez d'importer un groupe fédéré, vous avez ["fédération des identités configurée"](#) et le groupe fédéré existe déjà dans le référentiel d'identité configuré.
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour ["synchronisation des groupes de locataires et des utilisateurs"](#), et vous êtes connecté à la grille source du locataire.

Accédez à l'assistant de création de groupe

Pour la première étape, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au Gestionnaire de locataires, bien qu'ils puissent utiliser les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.

- **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.



Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **nom unique** existe déjà pour le locataire sur la grille de destination.

- **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l'attribut `sAMAccountName`. Pour OpenLDAP, le nom unique est le nom associé à l'attribut `uid`.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :

- **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.
- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

Voir "[Autorisations de gestion des locataires](#)".

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposent les utilisateurs.

Étapes

1. Sélectionnez la stratégie que vous souhaitez utiliser pour ce groupe.

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Réduction des ransomwares	Cet exemple de règle 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 des objets des compartiments pour lesquels la gestion des versions d'objet est activée. Les utilisateurs de tenant Manager disposant de l'autorisation gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

Pour plus d'informations sur les stratégies de groupe, notamment la syntaxe de la langue et des exemples, reportez-vous à la section "[Exemples de stratégies de groupe](#)".

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux qui existent déjà.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer groupe** et **Terminer**.

Le groupe que vous avez créé apparaît dans la liste des groupes.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles** et que vous êtes sur la grille source du locataire, le nouveau groupe est synchronisé avec la grille de destination du locataire. **Réussi** apparaît comme statut de synchronisation dans la section Vue d'ensemble de la page de détails du groupe.

Autorisations de gestion des locataires StorageGRID

Avant de créer un groupe de locataires, tenez compte des autorisations que vous souhaitez attribuer à ce groupe. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Un utilisateur peut appartenir à un ou plusieurs groupes. Les autorisations sont cumulatives si un utilisateur appartient à plusieurs groupes.

Pour vous connecter au Gestionnaire de locataires ou utiliser l'API de gestion des locataires, les utilisateurs doivent appartenir à un groupe disposant d'au moins une autorisation. Tous les utilisateurs autorisés à se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Modifier son propre mot de passe (pour les utilisateurs locaux)

Pour toutes les autorisations, le paramètre mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctions associés.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Vous pouvez attribuer les autorisations suivantes à un groupe.

Autorisations	Description	Détails
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires.	
Gérez vos identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu STORAGE (S3) > My S3 Access keys .

Autorisations	Description	Détails
Afficher tous les compartiments	Permet aux utilisateurs d'afficher tous les buckets et configurations de buckets.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu compartiments. 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.
Gestion de tous les compartiments	Permet aux utilisateurs d'utiliser Tenant Manager et l'API Tenant Management pour créer et supprimer des compartiments S3 et pour gérer les paramètres de tous les compartiments S3 du compte locataire, quels que soient les compartiments S3 ou les stratégies de groupe.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu compartiments. 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.
Gestion des terminaux	Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu Platform Services Endpoints .
Utilisez l'onglet de la console S3	Associé à l'autorisation Afficher tous les compartiments ou gérer tous les compartiments, permet aux utilisateurs d'afficher et de gérer des objets à partir de l'onglet de la console S3 de la page de détails d'un compartiment.	

Gérer les groupes de locataires StorageGRID

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, etc.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).

Afficher ou modifier un groupe

Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Consultez les informations fournies sur la page groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte de tenant.

Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez des groupes sur la grille source du locataire :

- Si certains groupes n'ont pas été synchronisés avec le locataire sur la grille de destination, suivez les étapes pour [Réessayer une synchronisation de groupe](#).
3. Si vous souhaitez modifier le nom du groupe :
 - a. Cochez la case du groupe.
 - b. Sélectionnez **actions > Modifier le nom du groupe**.
 - c. Saisissez le nouveau nom.
 - d. Sélectionnez **Enregistrer les modifications**.
 4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
 - Sélectionnez le nom du groupe.
 - Cochez la case du groupe et sélectionnez **actions > Afficher les détails du groupe**.
 5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :
 - Nom d'affichage
 - Nom unique
 - Type
 - Mode d'accès
 - Autorisations
 - Règle S3
 - Nombre d'utilisateurs dans ce groupe
 - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :
 - État de la synchronisation, soit **Réussie** soit **Échec**
 - Pour les groupes fédérés, une bannière bleue indique 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. Se référer à "[Créez des groupes pour un locataire S3](#)" pour plus de détails sur ce qu'il faut saisir.
 - a. Dans la section Vue d'ensemble, modifiez le nom d'affichage en sélectionnant le nom ou l'icône de modification .
 - b. Dans l'onglet **autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
 - c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.

Sélectionnez éventuellement une autre stratégie de groupe S3 ou saisissez la chaîne JSON d'une stratégie personnalisée selon vos besoins.

7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :

a. Sélectionnez l'onglet utilisateurs.

Username	Full name	Denied access
User_02	User_02_Managers	No

b. Sélectionnez **Ajouter des utilisateurs**.

c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

Un message de réussite s'affiche en haut à droite.

8. Pour supprimer des utilisateurs locaux du groupe :

a. Sélectionnez l'onglet utilisateurs.

b. Sélectionnez **Supprimer utilisateurs**.

c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

Un message de réussite s'affiche en haut à droite.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer le groupe

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera synchronisé avec la grille de destination du locataire.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions > Dupliquer le groupe**.
4. Voir "[Créer des groupes pour un locataire S3](#)" pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer groupe**.

Réessayer la synchronisation des groupes

Si la synchronisation d'un groupe échoue, la mention « Échec » s'affiche dans la colonne « État de la synchronisation » du groupe. Une bannière apparaît au-dessus du tableau pour indiquer qu'un ou plusieurs groupes ont échoué à se synchroniser.

Étapes

Pour réessayer la synchronisation :

1. Sur la bannière, sélectionnez **Réessayer la synchronisation**. Cette opération relance la synchronisation pour tous les groupes qui n'ont pas pu être synchronisés.
2. Pour réessayer la synchronisation d'un groupe, sélectionnez le nom du groupe. Sur la page des détails du groupe, sélectionnez **Réessayer la synchronisation**.
3. Consultez l'état de l'opération de synchronisation sur la page de détails de chaque groupe que vous synchronisez.

Si la nouvelle tentative réussit, la mention « Succeeded » apparaît dans la colonne « Sync status » pour chaque groupe synchronisé avec succès, et la bannière disparaît.

Pour plus d'informations, voir ["Synchroniser les groupes de locataires et les utilisateurs"](#).

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de tenant ni utiliser le compte de tenant.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions > Supprimer groupe** ou **actions > Supprimer groupes**.

Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Configurer AssumeRole

Avant de commencer

Vous devez être administrateur pour configurer AssumeRole.

Description de la tâche

Pour configurer AssumeRole, créez le groupe cible à assumer, si le groupe n'existe pas déjà. Modifiez la politique S3 du groupe pour spécifier les actions autorisées pour assumer ce groupe. Modifiez la politique de confiance S3 du groupe pour spécifier les utilisateurs de confiance autorisés à assumer le groupe avec l'API AssumeRole.

Les informations d'identification de sécurité temporaires créées en supposant que ce groupe est valide pour une durée limitée. La séance dure entre 15 minutes et 12 heures, et la séance par défaut est de 1 heure. Lorsque vous supprimez l'utilisateur de la politique de confiance S3 du groupe, l'utilisateur ne peut plus assumer ce groupe.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Sélectionnez le nom du groupe.
3. Sélectionnez l'onglet **Politique de confiance S3**.
4. Ajoutez votre politique de confiance S3, y compris une liste d'utilisateurs pouvant exécuter AssumeRole.

5. Sélectionnez **Enregistrer les modifications**.
6. Sélectionnez l'onglet **Stratégie de groupe S3**.
7. Modifiez la politique S3 pour spécifier uniquement les actions S3 requises pour les utilisateurs de confiance ajoutés dans la politique de confiance S3 de ce groupe.
8. Sélectionnez **Enregistrer les modifications**.

Exemple de politique de confiance S3 AssumeRole

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

Le directeur :

- `"Principal": "*"` Correspond à tout le monde, y compris aux requêtes anonymes (non signées)
- `"Principal": { "AWS": "*" }` correspond à toute identité ou utilisateur authentifié (ne correspond pas aux requêtes anonymes)
- S'applique uniquement aux stratégies de compartiment
- Le principal est le ou les comptes/utilisateurs auxquels les autorisations sont accordées ou refusées

Une fois la configuration terminée, les utilisateurs répertoriés dans la politique de confiance S3 peuvent exécuter AssumeRole et recevoir des informations d'identification. Les autorisations finales sont déterminées par la politique de groupe, la politique de compartiment et la politique de session. ["Utiliser les politiques d'accès"](#) .

Gérer les utilisateurs locataires de StorageGRID

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux afin de définir les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Vous pouvez également importer des utilisateurs fédérés. Le Tenant Manager inclut 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 Tenant Manager ni à l'API de gestion des locataires, bien qu'ils puissent utiliser des applications clientes pour accéder aux ressources du locataire, en fonction des autorisations de groupe.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour ["synchronisation des groupes de locataires et des utilisateurs"](#), et vous êtes connecté à la grille source du locataire.

Créez un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **Gestion des accès > Utilisateurs**.
2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **entrer les informations d'identification de l'utilisateur**, renseignez les champs suivants.

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	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 locataire dispose de l'autorisation utiliser la connexion de fédération de grille, une erreur de clonage se produit si le même Nom d'utilisateur existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.

Champ	Description
Refuser l'accès	Sélectionnez Oui pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez Oui pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Attribuez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'ils peuvent effectuer.

L'attribution d'un utilisateur à des groupes est facultative. Si vous le souhaitez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

Les utilisateurs qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposent de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "[Autorisations de gestion des locataires](#)".

2. Sélectionnez **Créer utilisateur**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est synchronisé avec la grille de destination du locataire. **Réussi** apparaît comme **État de la synchronisation** dans la section Vue d'ensemble de la page de détails de l'utilisateur.

3. Sélectionnez **Terminer** pour revenir à la page utilisateurs.

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **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 pour ce compte de tenant.

3. Si vous souhaitez modifier le nom complet de l'utilisateur :

- Cochez la case de l'utilisateur.
- Sélectionnez **actions > Modifier le nom complet**.
- Saisissez le nouveau nom.
- Sélectionnez **Enregistrer les modifications**.

4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :

- Sélectionnez le nom d'utilisateur.
- Cochez la case de l'utilisateur et sélectionnez **actions > Afficher les détails de l'utilisateur**.

5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :

- Nom complet

- Nom d'utilisateur
 - Type d'utilisateur
 - Accès refusé
 - Mode d'accès
 - Appartenance à un groupe
6. Modifiez les paramètres utilisateur selon vos besoins. Voir [Créer un utilisateur local](#) pour plus de détails sur ce que vous devez saisir.
- a. Dans la section Vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .
- Vous ne pouvez pas modifier le nom d'utilisateur.
- b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.
 - c. Dans l'onglet **accès**, sélectionnez **non** pour permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
 - d. Dans l'onglet **clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "[Création des clés d'accès S3 d'un autre utilisateur](#)".
 - e. Dans l'onglet **groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Sélectionnez ensuite **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Importer des utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

Étapes

1. Sélectionnez **Gestion des accès > Utilisateurs**.
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou plusieurs utilisateurs fédérés.

Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

- a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
- b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Importer les utilisateurs fédérés**.

Après avoir fermé la boîte de dialogue **Importer les utilisateurs fédérés**, les informations sur les utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

Dupliquer l'utilisateur local

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** et que vous dupliquez un utilisateur à partir de la grille source du locataire, l'utilisateur dupliqué sera synchronisé avec 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 utilisateur**.
4. Voir [Créer un utilisateur local](#) pour plus de détails sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Réessayer la synchronisation des utilisateurs

Si la synchronisation échoue pour un utilisateur, la mention « Échec » s'affiche dans la colonne « État de la synchronisation » de cet utilisateur. Une bannière apparaît au-dessus du tableau pour indiquer qu'un ou plusieurs utilisateurs ont échoué à se synchroniser.

Étapes

Pour réessayer la synchronisation :

1. Sur la bannière, sélectionnez **Réessayer la synchronisation**. Cette opération relance la synchronisation pour tous les utilisateurs dont la synchronisation a échoué.
2. Pour réessayer la synchronisation d'un utilisateur, sélectionnez le nom de l'utilisateur. Sur la page des détails de l'utilisateur, sélectionnez **Réessayer la synchronisation**.
3. Consultez l'état de l'opération de synchronisation sur la page de détails de chaque utilisateur que vous synchronisez.

Si la nouvelle tentative réussit, « Réussi » apparaît dans la colonne « État de la synchronisation » pour chaque utilisateur synchronisé avec succès, et la bannière disparaît.

Pour plus d'informations, voir "[Synchroniser les groupes de locataires et les utilisateurs](#)".

Supprimez un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte de locataire StorageGRID.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles** et que vous supprimez un utilisateur local, StorageGRID supprimera l'utilisateur correspondant sur les autres grilles de la connexion, sauf s'il s'agit d'un utilisateur fédéré sur une grille cible. 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 à supprimer.

3. Sélectionnez **actions > Supprimer utilisateur** ou **actions > Supprimer utilisateurs**.

Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer utilisateur** ou **Supprimer utilisateurs**.

Gestion des clés d'accès S3

Gérer les clés d'accès S3 dans StorageGRID

Chaque utilisateur d'un compte de locataire S3 doit disposer d'une clé d'accès pour stocker et récupérer des objets dans le système StorageGRID. Une clé d'accès se compose d'un ID de clé d'accès et d'une clé d'accès secrète.

Les clés d'accès S3 peuvent être gérées de la manière suivante :

- Les utilisateurs disposant de l'autorisation **gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Root Access** peuvent gérer les clés d'accès du compte root S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

StorageGRID prend en charge l'authentification Signature version 2 et Signature version 4. L'accès entre comptes n'est pas autorisé sauf si cette règle est explicitement activée par une règle de compartiment.

Créez vos propres clés d'accès S3 dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer vos propres clés d'accès S3. Vous devez disposer d'une clé d'accès pour accéder à vos compartiments et objets.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez vos propres informations d'identification S3 ou autorisations d'accès racine"](#).

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec votre nouvel ID de clé d'accès et votre clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n'utilisez pas. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez une durée d'expiration pour vos clés afin de limiter votre accès à une certaine période. La définition d'un délai d'expiration court peut vous aider à réduire le risque si votre ID de clé d'accès et votre clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer

régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour vos clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3) > Mes clés d'accès**.

La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer clé**.

3. Effectuez l'une des opérations suivantes :

- Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
- Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.



La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

4. Sélectionnez **Créer une clé d'accès**.

La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de votre ID de clé d'accès et de votre clé secrète d'accès.

5. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.



Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

La nouvelle clé apparaît sur la page Mes clés d'accès.

Consultez vos clés d'accès S3 dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez de la "[autorisation appropriée](#)", vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, vous pouvez "[créer de nouvelles clés](#)" ou "[supprimer les clés](#)" que vous n'utilisez plus.



Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs possédant les informations d'identification Manage Your Own S3 ["permission"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Mes clés d'accès**.
2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez les clés que vous n'utilisez plus.

Si vous créez de nouvelles clés avant l'expiration des clés existantes, vous pouvez commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3 dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérez vos propres identifiants S3"](#).



Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3) > Mes clés d'accès**.
2. Sur la page Mes clés d'accès, cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Créez les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un locataire S3 avec l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme les applications qui ont besoin d'accéder à des compartiments et des objets.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#).

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour les autres utilisateurs afin qu'ils puissent créer et gérer des compartiments pour leur compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que les besoins de l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez un délai d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une certaine période. La définition d'un délai d'expiration court peut aider à réduire le risque si l'ID de clé d'accès et la clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour les clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **Gestion des accès > Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis **touche Créer**.
4. Effectuez l'une des opérations suivantes :
 - Sélectionnez **ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
 - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.



La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

5. Sélectionnez **Créer une clé d'accès**.

La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de l'ID de clé d'accès et de la clé secrète.

6. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.



Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée dans l'onglet touches d'accès de la page des détails de l'utilisateur.

Afficher les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par heure d'expiration pour déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).



Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **Gestion des accès > Utilisateurs**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Dans la page Détails de l'utilisateur, sélectionnez **touches d'accès**.
4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

Si vous créez de nouvelles clés avant l'expiration des clés existantes, l'utilisateur peut commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

Les clés expirées sont supprimées automatiquement.

Informations associées

- ["Créez les clés d'accès S3 d'un autre utilisateur"](#)
- ["Supprimez les clés d'accès S3 d'un autre utilisateur"](#)

Supprimer les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).



Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **Gestion des accès > Utilisateurs**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **touches d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions > Supprimer la touche sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Gestion des compartiments S3

Créez un compartiment StorageGRID S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès racine ou de la fonction gérer tous les compartiments ["permission"](#). Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.



Les autorisations 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 règle de groupe"](#).

- Si vous prévoyez d'activer le verrouillage objet S3 pour un compartiment, un administrateur du grid a activé le paramètre de verrouillage objet S3 global pour le système StorageGRID. Vous avez également passé en revue les exigences relatives aux compartiments et aux objets S3 Object Lock.

- Si plusieurs locataires disposent chacun de jusqu'à 5 000 compartiments, chaque nœud de stockage de la grille possède un minimum de 64 Go de RAM.



Le système StorageGRID prend en charge un maximum de 20 000 compartiments par compte locataire S3. Chaque grille peut contenir jusqu'à 100 000 compartiments, y compris "seaux de branches". Il existe également une limite pour "profondeur du compartiment de branche".

Accéder à l'assistant

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez **Créer un compartiment**.

Entrez les détails

Étapes

1. Entrez les détails du compartiment.

Champ	Description
Nom du compartiment	Nom du compartiment conforme aux règles suivantes : • Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). • Doit être conforme DNS. • Doit contenir au moins 3 et 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. • Ne doit pas contenir de périodes dans les demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, veuillez consulter la "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". Remarque : vous ne pouvez pas modifier le nom du compartiment après avoir créé le compartiment.

Champ	Description
Région	La région du godet. 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 <code>us-east-1</code> région. Si la région par défaut est configurée sur une région autre que <code>us-east-1</code>, cette autre région est initialement sélectionnée dans la liste déroulante. Remarque : vous ne pouvez pas modifier la région après avoir créé le compartiment.

2. Sélectionnez **Continuer**.

Gérer les paramètres

Étapes

1. Activez éventuellement le contrôle de version d'objet pour le compartiment.

Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire.

Vous devez activer le contrôle de version des objets si :

- Le bucket sera utilisé pour la réplication inter-grille.
- Vous souhaitez créer un "seau de branche" de ce seau.

2. Si le paramètre global S3 Object Lock est activé, activez éventuellement S3 Object Lock pour que le compartiment stocke des objets à l'aide d'un modèle WORM (Write-once-read-many).

Activez le verrouillage des objets S3 pour un compartiment uniquement si vous devez conserver les objets pendant une durée fixe, par exemple, pour répondre à certaines exigences réglementaires. Le verrouillage objet S3 est un paramètre permanent qui vous permet d'empêcher la suppression ou l'écrasement d'objets pendant une durée fixe ou indéfiniment.



Une fois le paramètre S3 Object Lock activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter à ce compartiment des objets qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ou le compartiment lui-même.

Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, vous pouvez activer **rétenion par défaut** pour ce compartiment.



Votre administrateur de grille doit vous donner l'autorisation de "Utiliser les fonctionnalités spécifiques du verrouillage objet S3".

Lorsque **Default Retention** est activé, les nouveaux objets ajoutés au compartiment sont automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **rétenion par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de rétention.

a. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La gouvernance	• Les utilisateurs disposant de l'`s3:BypassGovernanceRetention` autorisation peuvent utiliser l'`x-amz-bypass-governance-retention: true` en-tête de la demande pour contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. Remarque : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

b. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le tenant, telle que définie par l'administrateur de la grille.

Une période de rétention *maximum*, qui peut être de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de rétention *default*, elle ne peut pas dépasser la valeur définie pour la période de rétention maximale. Si nécessaire, demandez à votre administrateur de grille d'augmenter ou de réduire la période de rétention maximale.

4. Vous pouvez également sélectionner **Activer la limite de capacité**, saisir une valeur et sélectionner l'unité de capacité.

La limite de capacité est la capacité maximale disponible pour les objets de ce compartiment. 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 godet est illimitée. Pour plus d'informations, reportez-vous à la section "[Utilisation limitée de la capacité](#)".

5. Si vous le souhaitez, sélectionnez **Activer la limite du nombre d'objets**.

La limite du nombre d'objets est le nombre maximal d'objets que ce bucket peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.

6. Sélectionnez **Créer un compartiment**.

Le godet est créé et ajouté au tableau sur la page godets.

- Si vous le souhaitez, sélectionnez **aller à la page des détails du compartiment** pour "[afficher les détails du compartiment](#)" effectuer une configuration supplémentaire.

Vous pouvez également "[créer des compartiments de branches](#)" selon les besoins.

Afficher les détails du compartiment S3 dans StorageGRID

Vous pouvez afficher les compartiments de votre compte de locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments](#)". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

- Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

La page compartiments s'affiche.

- Consultez le tableau récapitulatif pour chaque compartiment.

Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.



Les valeurs nombre d'objets, espace utilisé et utilisation affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds. Si la gestion des versions des compartiments est activée, les versions des objets supprimés sont incluses dans le nombre d'objets.

Nom

Nom unique du compartiment, qui ne peut pas être modifié.

Fonctionnalités activées

Liste des fonctions activées pour le compartiment.

Verrouillage d'objet S3

Indique si le verrouillage d'objet S3 est activé pour le compartiment.

Cette colonne apparaît uniquement si le verrouillage objet S3 est activé pour la grille. Cette colonne affiche également des informations pour tous les compartiments conformes existants.

Région

La région du compartiment, qui ne peut pas être modifiée. Cette colonne est masquée par défaut.

Nombre d'objets

Nombre d'objets dans ce compartiment. Si la gestion des versions des compartiments est activée, les versions d'objets non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, il est possible que cette valeur ne soit pas mise à jour immédiatement.

Espace utilisé

Taille logique de tous les objets du compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou avec code d'effacement, ni pour les métadonnées d'objet.

La mise à jour de cette valeur peut prendre jusqu'à 10 minutes.

Du stockage

Pourcentage utilisé de la limite de capacité du godet, si un pourcentage a été défini.

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 elle est définie) lorsqu'un locataire commence à télécharger des objets et rejette de nouvelles iningests dans ce compartiment si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lorsqu'il détermine si la limite de capacité a été dépassée. En cas de suppression d'objets, un locataire peut temporairement empêcher le chargement de nouveaux objets dans ce compartiment 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 au stockage des objets et de leurs métadonnées.

Capacité

S'il est défini, la limite de capacité du godet.

Date de création

Date et heure de création du compartiment. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.
 - a. Affichez le récapitulatif en haut de la page Web pour confirmer les détails du compartiment, tels que le nombre de régions et d'objets.
 - b. Affichez les barres d'utilisation de la limite de capacité et de la limite du nombre d'objets. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.
 - c. Au besoin, sélectionnez **Supprimer les objets dans le compartiment** et **Supprimer le compartiment**.



Soyez attentif aux mises en garde qui apparaissent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, se reporter à :

- ["Supprime tous les objets d'un compartiment"](#)
- ["Supprimer un compartiment"](#) (le godet doit être vide)

- d. Afficher ou modifier les paramètres du compartiment dans chacun des onglets, selon les besoins.
 - **S3 Console** : permet d'afficher les objets du compartiment. Pour plus d'informations, reportez-vous ["Utiliser la console S3"](#) à .
 - **Options de compartiment** : afficher ou modifier les paramètres des options. Certains paramètres, tels que S3 Object Lock, ne peuvent pas être modifiés après la création du compartiment.
 - ["Gestion de la cohérence des compartiments"](#)
 - ["Mises à jour de l'heure du dernier accès"](#)

- ["Limite de capacité"](#)
- ["Limite du nombre d'objets"](#)
- ["Gestion des versions d'objet"](#)
- ["Verrouillage d'objet S3"](#)
- ["Rétention de compartiments par défaut"](#)
- ["Gérer la réplication entre les grilles"](#) (si autorisé pour le locataire)
- **Platform services:** ["Gestion des services de plateforme"](#) (Si autorisé pour le locataire)
- **Accès au compartiment :** afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
 - Configure ["CORS pour les buckets et les objets"](#) 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 compartiment S3 et les objets dans ce compartiment.
- **Branches :** afficher la liste des branches du bucket. ["Créer un nouveau bucket de branches ou gérer des buckets de branches"](#) .

Découvrez les compartiments de branche StorageGRID

Un bucket de branche fournit un accès aux objets d'un bucket tels qu'ils existaient à un moment donné.

Vous créez un bucket de branche à partir d'un bucket existant. Une fois que vous avez créé un bucket de branche, le bucket d'origine à partir duquel il a été créé est appelé le *bucket de base*. De plus, vous pouvez créer un bucket de branche à partir d'un autre bucket de branche.

Un bucket de branche fournit un accès aux données protégées, mais ne sert pas de sauvegarde. Pour continuer à protéger les données, utilisez ces fonctionnalités sur les buckets de base :

- ["Verrouillage d'objet S3"](#)
- ["Réplication entre plusieurs grilles"](#) pour les godets de base
- ["Politiques de compartiments"](#) pour les buckets versionnés pour nettoyer les anciennes versions d'objets

Notez les caractéristiques suivantes des compartiments de branche :

- Vous pouvez accéder aux objets dans les compartiments de branche en utilisant ["Console S3 pour télécharger des objets"](#) .
- Lorsque les clients accèdent aux objets d'un bucket de branche, le bucket de branche ["politiques d'accès"](#) , plutôt que les politiques du compartiment de base, déterminent si l'accès est accordé ou refusé.
- Les objets créés dans un bucket de base sont évalués en fonction de la manière dont ["Règles ILM"](#) appliquer au bucket de base. Les objets créés dans un bucket de branche sont évalués en fonction de la manière dont les règles ILM s'appliquent au bucket de branche.
- La réplication inter-grille n'est pas prise en charge pour les buckets de branche.
- Les services de plateforme ne sont pas pris en charge pour les buckets de branches.

Exemples d'utilisation de compartiments de branchement

- Vous pouvez utiliser un bucket de branche pour supprimer les objets corrompus en créant un bucket de branche à partir d'un moment antérieur à la corruption, puis en pointant les applications vers le bucket de branche au lieu du bucket de base qui contient les objets corrompus.
- Vous enregistrez des données dans un bucket versionné. Une vulnérabilité accidentelle a provoqué l'ingestion de nombreux objets indésirables après le temps T . Vous pouvez créer un compartiment de branche pour la valeur Avant l'heure, T , et rediriger les opérations client vers ce compartiment de branche. Ensuite, seuls les objets ingérés avant l'heure Avant T sont exposés aux clients.
- Vous enregistrez des données dans un compartiment versionné. Une vulnérabilité accidentelle a entraîné l'ingestion de nombreux objets indésirables entre les instants $T1$ et $T2$. Vous pouvez créer un compartiment de branche pour les valeurs temporelles *Exclude*, $T1$ et $T2$, et rediriger les opérations client vers ce compartiment de branche. Ainsi, seuls les objets ingérés avant $T1$ et après $T2$ sont exposés aux clients.

Opérations sur les objets dans les compartiments de branche

- Une opération d'objet PUT sur un bucket de branche crée un objet dans la branche.
- Une opération d'objet GET sur un bucket de branche récupère un objet de la branche. Si l'objet n'existe pas dans le bucket de branche, l'objet est récupéré à partir du bucket de base.
- Les suppressions d'objets des compartiments de branche se produisent comme suit :

Fonctionnement	Cible	Résultat	Visibilité des objets dans le bucket de base	Visibilité des objets dans le bucket de branche
Supprimer sans ID de version	Godet de base	Le marqueur de suppression est créé uniquement pour le compartiment de base	HEAD/GET renvoie L'objet n'existe pas, mais des versions spécifiques sont toujours accessibles	HEAD/GET renvoie L'objet existe et des versions spécifiques sont toujours accessibles Le marqueur de suppression aurait été créé après le bucket de branche <code>beforeTime</code> .
Supprimer avec l'ID de version	Godet de base	La version d'objet spécifique est supprimée pour le bucket de base et de branche	HEAD/GET renvoie La version de l'objet n'existe pas	HEAD/GET renvoie La version de l'objet n'existe pas
Supprimer sans ID de version	Seau à branches	Le marqueur de suppression est créé uniquement pour le compartiment de branche	HEAD/GET renvoie l'objet (l'objet bucket de base n'est pas affecté)	HEAD/GET renvoie L'objet n'existe pas

Fonctionnement	Cible	Résultat	Visibilité des objets dans le bucket de base	Visibilité des objets dans le bucket de branche
Supprimer avec l'ID de version	Seau à branches	La version d'objet spécifique est supprimée uniquement pour le bucket de branche	HEAD/GET renvoie une version d'objet spécifique (l'objet de compartiment de base n'est pas affecté)	HEAD/GET renvoie La version de l'objet n'existe pas

Voir aussi "[Suppression d'objets avec version S3](#)".

Gérer les compartiments de branche StorageGRID

Utilisez le gestionnaire de locataires pour créer et afficher les détails des compartiments de branches.

Avant de commencer

- Vous vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès Root ou "[Autorisations de gestion de tous les compartiments](#)". Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le bucket de base à partir duquel vous souhaitez créer une branche a "[contrôle de version activé](#)".
- Vous êtes le propriétaire du bucket de base.

Description de la tâche

Notez les informations suivantes pour les compartiments de branches :

Limite de profondeur du compartiment de branche

Un compartiment de branche peut contenir jusqu'à 20 compartiments de base. À mesure que la profondeur des compartiments de branche augmente, la latence d'accès à S3 peut également augmenter, en particulier pour les appels ListObjectVersions.

- Si vous créez un compartiment de branche à partir d'un compartiment de base qui est un compartiment standard (un compartiment initialement créé comme compartiment de base), le nouveau compartiment de branche possède un seul compartiment de base.
- Si le compartiment de base est lui-même un compartiment de branche, le nouveau compartiment de branche hérite de tous les compartiments de base de ce compartiment de branche. L'utilisateur ne spécifie directement qu'un seul compartiment de base ; les compartiments de base hérités sont implicites.
- Le nombre total de compartiments de base (explicites et implicites) ne peut pas dépasser 20.

Par exemple, supposons que le compartiment **A** soit un compartiment standard avec le versionnage activé :

- Le compartiment de branche **B**, créé à partir de **A**, a un compartiment de base : **A**.
- Le compartiment de branche **C**, créé à partir de **B**, possède deux compartiments de base : **B** (explicite) et **A** (implicite).
- Le compartiment de branche **D**, créé à partir de **C**, possède trois compartiments de base : **C**

(explicite), **B** (implicite) et **A** (implicite).

- Ce schéma se poursuit jusqu'à une profondeur maximale de 20 seaux de base.

Autorisations de verrouillage d'objet S3

Les autorisations permettant de définir les propriétés de verrouillage d'objets S3 des compartiments ou des objets peuvent être accordées par "[politique de compartiment ou règle de groupe](#)".

Versionnage suspendu

Si vous suspendez le contrôle de version sur le bucket de base, le contenu du bucket de base ne sera plus visible dans ses buckets de branche.



Après avoir configuré et créé un bucket de branche, vous ne pouvez pas modifier la configuration.

Créer un bucket de branche

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le bucket à partir duquel vous souhaitez créer une branche (le « bucket de base »).
3. Sur la page des détails du bucket, sélectionnez **Branches > Créer un bucket de branche**.

Le bouton **Créer un bucket de branche** est désactivé si le contrôle de version n'est pas activé pour le bucket de base.

Entrez les détails

Étapes

1. Saisissez les détails du compartiment de branche.

Champ	Description
Nom du bucket de branche	Un nom pour le bucket de branche qui respecte ces règles : • Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). • Doit être conforme DNS. • Doit contenir au moins 3 et 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. • Ne doit pas contenir de périodes dans les demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, voir "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". Remarque : vous ne pouvez pas modifier le nom après avoir créé le bucket de branche.
Région (ne peut pas être modifiée pour les compartiments de branche)	La région du bucket de branche. La région du bucket de branche doit correspondre à la région du bucket de base, ce champ est donc désactivé pour les buckets de branche.
Type de godet de branche	• Lecture-écriture : Vous pouvez ajouter ou supprimer des objets ou des versions d'objets dans le bucket de branche. • Lecture seule : vous ne pouvez pas modifier les objets dans le bucket de branche. Remarque : vous pouvez définir le type de compartiment de branche en lecture seule uniquement si le compartiment de branche est vide. Si le type d'un bucket de branche existant est défini sur lecture-écriture et que vous n'y avez pas écrit, vous pouvez modifier le type en lecture seule.

2. Sélectionnez **Continuer**.

Filtre temporel

Choisissez la plage horaire à inclure pour les versions d'objets du compartiment de base. Pour tout filtre temporel, sélectionnez une date dans la plage suivante :

- Date minimale : 1er janvier 2010 (UTC)
- Date maximale : cinq ans à compter d'aujourd'hui (UTC)

Avant

Le compartiment de branche permet d'accéder aux versions d'objets créées avant l'heure *Before*.

Après

Le compartiment de branche permet d'accéder aux versions d'objets créées après l'heure *After*.

Entre

Le compartiment de branche permet d'accéder aux versions d'objets créées entre les heures *From* et *To*.

Exclure

Le compartiment de branche ne donne pas accès aux versions d'objets créées entre les heures *Exclude from* et *Exclude to*.

Gérer les paramètres de l'objet (facultatif)

Les paramètres d'objet pour un bucket de branche n'affectent pas les versions d'objet dans le bucket de base.

Étapes

1. Si le paramètre global de verrouillage d'objet S3 est activé, activez éventuellement le verrouillage d'objet S3 pour le compartiment de branche. Pour activer le verrouillage d'objet S3, le bucket de branche doit être un bucket en lecture-écriture.

Activez le verrouillage d'objet S3 pour un compartiment de branche 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 au bucket de branche qui ne peuvent pas être modifiés. Vous ne pourrez peut-être pas supprimer ces objets ni le bucket de branche lui-même.

2. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, activez éventuellement la **Rétention par défaut** pour le bucket de branche.



Votre administrateur de grille doit vous donner l'autorisation de "[Utiliser les fonctionnalités spécifiques du verrouillage objet S3](#)".

Lorsque la **rétention par défaut** est activée, les nouveaux objets ajoutés au bucket de branche 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 de branche.

Mode de rétention par défaut	Description
La gouvernance	- Les utilisateurs disposant de l'`s3:BypassGovernanceRetention` autorisation peuvent utiliser l'`x-amz-bypass-governance-retention: true` en-tête de la demande pour contourner les paramètres de rétention. - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
La conformité	- L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. Remarque : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

- b. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket de branche.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés au bucket de branche 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 rétention *maximum*, qui peut être de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de rétention *default*, elle ne peut pas dépasser la valeur définie pour la période de rétention maximale. Si nécessaire, demandez à votre administrateur de grille d'augmenter ou de réduire la période de rétention maximale.

3. En option, sélectionnez **Activer la limite de capacité**.

La limite de capacité est la capacité maximale disponible pour le bucket de branche. 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 du bucket de branche est illimitée. Consultez "[Utilisation limitée de la capacité](#)" pour plus d'informations.



Ce paramètre s'applique uniquement aux objets directement ingérés dans le bucket de branche, et non aux objets visibles depuis le bucket de base via le bucket de branche.

4. En option, sélectionnez **Activer la limite du nombre d'objets**.

La limite du nombre d'objets est le nombre maximal d'objets que le bucket de branche peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.



Ce paramètre s'applique uniquement aux objets directement ingérés dans le bucket de branche, et non aux objets visibles depuis le bucket de base via le bucket de branche.

5. Sélectionnez **Créer un compartiment**.

Le bucket de branche est créé et ajouté à la table sur la page Buckets.

6. En option, sélectionnez **Accéder à la page des détails du bucket** pour "[afficher les détails du bucket de branche](#)" et effectuer une configuration supplémentaire.

Sur la page Détails du bucket, certaines options de configuration liées à la modification des objets sont désactivées pour les buckets en lecture seule.

Appliquer une étiquette de stratégie ILM à un compartiment StorageGRID

Vous pouvez choisir une balise de règle ILM à appliquer à un compartiment en fonction de vos besoins en stockage objet.

La politique ILM contrôle l'emplacement du stockage des données objet et leur suppression au bout d'une période donnée. Votre administrateur du grid crée des règles ILM et les attribue aux balises de règles ILM lors de l'utilisation de plusieurs règles actives.



Évitez de fréquemment réaffecter le tag de stratégie d'un compartiment. Sinon, des problèmes de performances risquent de se produire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments](#)". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

La page compartiments s'affiche. Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.

2. Sélectionnez le nom du compartiment auquel vous souhaitez attribuer une balise de règle ILM.

Vous pouvez également modifier l'affectation de balises de stratégie ILM pour un compartiment auquel une balise est déjà attribuée.



Les valeurs nombre d'objets et espace utilisé affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds. Si la gestion des versions des compartiments est activée, les versions des objets supprimés sont incluses dans le nombre d'objets.

3. Dans l'onglet Options de compartiment, développez la balise de stratégie ILM accordéon. 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

compartiment.



La modification de la balise de règle ILM d'un compartiment déclenche la réévaluation des règles ILM de tous les objets du compartiment. Si la nouvelle règle conserve des objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à l'étiquette que vous souhaitez affecter au compartiment.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie dans le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de règle ILM.



Assurez-vous que vos applications S3 ne remplacent pas accidentellement ou ne suppriment pas la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au compartiment, les objets du compartiment seront de nouveau évalués par rapport à la règle ILM par défaut.



Définissez et modifiez les balises de règles ILM à l'aide uniquement du gestionnaire de locataires ou de l'API du gestionnaire de locataires sur lequel la balise de règle ILM est validée. Ne modifiez pas la `NTAP-SG-ILM-BUCKET-TAG` balise de stratégie ILM à l'aide de l'API S3 `PutBucketTagging` ou de l'API S3 `DeleteBucketTagging`.



La modification de la balise de règle attribuée à un compartiment a un impact temporaire sur les performances, tandis que la réévaluation des objets est effectuée à l'aide de la nouvelle règle ILM.

Gérer la politique du compartiment StorageGRID

Vous pouvez contrôler l'accès utilisateur à un compartiment S3 et aux objets de ce compartiment.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès racine"](#). Les autorisations `Afficher tous les compartiments` et `Gérer tous les compartiments` permettent uniquement l'affichage.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres risquent de ne pas être disponibles.

Étapes

1. Sélectionnez **godets**, puis sélectionnez le compartiment que vous souhaitez gérer.
2. Sur la page de détails du compartiment, sélectionnez **accès au compartiment > Stratégie de compartiment**.
3. Effectuez l'une des opérations suivantes :
 - Entrez une stratégie de compartiment en cochant la case **Enable policy**. Entrez ensuite une chaîne au format JSON valide.

Chaque politique de compartiment a une taille limite de 20,480 octets.
 - Modifiez une règle existante en modifiant la chaîne.

- Désactivez une stratégie en désélectionnant **Activer la stratégie**.

Pour plus d'informations sur les règles de compartiment, notamment la syntaxe du langage et des exemples, reportez-vous à la section "[Exemples de politiques de compartiments](#)".

Gérer la cohérence des buckets StorageGRID

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de compartiment, ainsi que pour fournir un équilibre entre la disponibilité des objets au sein d'un compartiment et la cohérence de ces objets entre plusieurs 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 client puissent répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Instructions de cohérence des compartiments

La cohérence des compartiments détermine la cohérence des applications client qui affectent les objets au sein de ce compartiment S3. En général, vous devez utiliser la cohérence **Read-After-New-write** pour vos compartiments.

modifiez la cohérence des compartiments

Si la cohérence **Read-After-New-write** ne répond pas aux exigences de l'application client, vous pouvez modifier la cohérence en définissant la cohérence du compartiment ou en utilisant l'`Consistency-Control` en-tête. L'`Consistency-Control` en-tête remplace la cohérence du godet.



Lorsque vous modifiez la cohérence d'un compartiment, seuls les objets ingérés après la modification sont garantis pour respecter le paramètre révisé.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez **** accordéon**.
4. Sélectionnez une cohérence pour les opérations effectuées sur les objets de ce compartiment.
 - **Tous** : fournit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
 - **Strong-global** : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.
 - **Strong-site** : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.

- **Read-After-New-write** (par défaut) : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

5. Sélectionnez **Enregistrer les modifications**.

Que se passe-t-il lorsque vous modifiez les paramètres de compartiment

Les compartiments ont plusieurs paramètres qui affectent le comportement des compartiments et des objets dans ces compartiments.

Les paramètres de compartiment suivants utilisent la cohérence **strong** par défaut. Si au moins deux nœuds de stockage ne sont disponibles dans aucun site, ou si un site n'est pas disponible, toute modification de ces paramètres peut ne pas être disponible.

- ["Suppression du compartiment vide en arrière-plan"](#)
- ["Heure du dernier accès"](#)
- ["Cycle de vie des compartiments"](#)
- ["Politique des compartiments"](#)
- ["Balisage du compartiment"](#)
- ["Gestion des versions de compartiment"](#)
- ["Verrouillage d'objet S3"](#)
- ["Chiffrement des compartiments"](#)



La valeur de cohérence pour la gestion des versions des compartiments, le verrouillage objet S3 et le chiffrement des compartiments ne peut pas être définie sur une valeur qui n'est pas parfaitement cohérente.

Les paramètres de compartiment suivants n'utilisent pas une cohérence élevée et offrent une plus grande disponibilité en cas de modification. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

- ["Configuration des services de plate-forme : intégration de notification, réplication ou recherche"](#)
- ["Configurer StorageGRID CORS pour les buckets et les objets"](#)
- [Modifier la cohérence du compartiment](#)



Si la cohérence par défaut utilisée lors de la modification des paramètres de compartiment ne répond pas aux exigences de l'application client, vous pouvez modifier la cohérence à l'aide de l'en-tête de ["L'API REST S3"](#) ou en utilisant les ``reducedConsistency`` options ou de ``force`` ["API de gestion des locataires"](#).

Activer ou désactiver les mises à jour du temps d'accès dans StorageGRID

Les administrateurs du grid créent les règles de gestion du cycle de vie des informations d'un système StorageGRID. Ils ont la possibilité de spécifier la date d'accès de dernier

objet afin de déterminer si celui-ci doit être déplacé vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez activer ces règles en activant les mises à jour de l'heure du dernier accès pour les objets dans un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **Last Access Time** comme filtre avancé ou comme heure de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle. Voir "[Utiliser l'heure du dernier accès dans les règles ILM](#)" pour plus de détails.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Last Access Time est l'une des options disponibles pour l'instruction de placement **Reference Time** pour une règle ILM. La définition de l'heure de référence d'une règle sur l'heure du dernier accès permet aux administrateurs de la grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés (lus ou affichés) pour la dernière fois.

Par exemple, pour s'assurer que les objets récemment affichés restent dans un stockage plus rapide, un administrateur du grid peut créer une règle ILM spécifiant ce qui suit :

- Les objets récupérés au cours du mois dernier doivent rester sur les nœuds de stockage locaux.
- Les objets qui n'ont pas été récupérés au cours du dernier mois doivent être déplacés vers un emplacement hors site.

Par défaut, les mises à jour de l'heure du dernier accès sont désactivées. Si votre système StorageGRID inclut une règle ILM qui utilise l'option **Last Access Time** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle.



La mise à jour du dernier accès lors de l'extraction d'un objet peut réduire les performances du StorageGRID, en particulier pour les petits objets.

Un impact sur les performances se produit lors des mises à jour des temps de dernier accès, car StorageGRID doit effectuer ces étapes supplémentaires chaque fois que les objets sont récupérés :

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez ces objets à la file d'attente ILM pour une réévaluation des règles et règles ILM actuelles

Le tableau récapitule le comportement appliqué à tous les objets du compartiment lorsque l'heure du dernier accès est désactivée ou activée.

Type de demande

	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération des métadonnées d'un objet lorsqu'une opération HEAD est émise	Non	Non	Non	Non
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
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.
3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Last Access Time Updates**.
4. Activer ou désactiver les mises à jour des heures du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifier le versionnage des objets pour un compartiment S3 dans StorageGRID

Si vous utilisez un locataire S3, vous pouvez modifier l'état de gestion des versions des compartiments S3.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres risquent de ne pas être disponibles.

Description de la tâche

Vous pouvez activer ou suspendre la gestion des versions d'objet pour un compartiment. Une fois que vous avez activé la gestion des versions pour un compartiment, il ne peut plus revenir à un état sans version. Toutefois, vous pouvez suspendre le contrôle de version du compartiment.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : la gestion des versions est activée
- Suspendu : la gestion des versions a déjà été activée et est suspendue

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

- ["Gestion des versions d'objet"](#)
- ["Règles et règles ILM pour les objets avec version S3 \(exemple 4\)"](#)
- ["Comment supprimer les objets"](#)

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Object multiversion**.
4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

La gestion des versions d'objet doit rester activée pour un compartiment utilisé pour la réplication entre plusieurs grilles. Si le verrouillage d'objet S3 ou la conformité héritée est activée, les options **Object versionnage** sont désactivées.

Option	Description
Activez le contrôle des versions	Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire. Les objets qui se trouvent déjà dans le compartiment sont avec gestion de version lorsqu'ils sont modifiés par l'utilisateur.
Suspendre la gestion des versions	Suspendre la gestion des versions d'objet si vous ne souhaitez plus créer de nouvelles versions d'objet. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez S3 Object Lock pour conserver les objets dans StorageGRID

Vous pouvez utiliser le verrouillage objet S3 si les compartiments et les objets doivent respecter les exigences réglementaires en matière de conservation des données.



Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctions spécifiques de verrouillage d'objet S3.

Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objets S3 est activé pour un système StorageGRID, un compte locataire S3 peut créer des compartiments avec ou sans le verrouillage d'objets S3 activé. Lorsque l'option permettant d'autoriser le verrouillage d'objets S3 pour les compartiments existants est activée, un compte locataire S3 peut activer le verrouillage d'objets S3 pour un compartiment existant. Si un compartiment a le verrouillage d'objets S3 activé, le versionnage du compartiment est requis et est activé automatiquement. Après qu'un compte locataire S3 a activé le verrouillage d'objets S3 pour un compartiment nouveau ou existant, il ne peut plus être désactivé.

Un compartiment sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne possède de paramètres de conservation.

Un compartiment avec S3 Object Lock peut contenir des objets avec et sans paramètres de conservation spécifiés par les applications client S3. Certains objets ingérés auront des paramètres de conservation.

Un compartiment avec le verrouillage d'objet S3 et la rétention par défaut configurés peut avoir téléchargé des objets 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 conservation lorsque la conservation par défaut est configurée. Les objets existants sans paramètres de conservation d'objet ne sont pas affectés.

Modes de rétention

La fonction de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de conservation Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
 - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
 - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date** : Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.



Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, reportez-vous à ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#).

Paramètre de rétention par défaut pour les compartiments

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent spécifier les paramètres par défaut suivants pour le compartiment :

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent

pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Reportez-vous à "[Créer un compartiment S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs du grid et aux utilisateurs de locataires contiennent des tâches de haut niveau relatives à l'utilisation de la fonction S3 Object Lock.

Administrateur du grid

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID.
- Autoriser les utilisateurs à activer le verrouillage d'objets S3 pour les compartiments existants.
- Assurez-vous que les politiques de gestion du cycle de vie des informations (ILM) sont *conformes*; c'est-à-dire "[Exigences des compartiments avec le verrouillage objet S3 activé](#)"-dire qu'elles respectent le .
- Si nécessaire, autorisez un locataire à utiliser le mode de conservation Compliance. Sinon, seul le mode gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Considérations relatives aux compartiments et aux objets avec le verrouillage d'objet S3
- Au besoin, contactez un administrateur de grille pour activer l'un des paramètres suivants :
 - Verrouillage d'objet global S3
 - Autoriser l'activation du verrouillage d'objets S3 pour les compartiments existants
- Créez des compartiments avec le verrouillage d'objet S3 activé.
- Activez le verrouillage des objets S3 sur les compartiments existants.
- Vous pouvez également configurer les paramètres de conservation par défaut d'un compartiment :
 - Mode de conservation par défaut : gouvernance ou conformité, si l'administrateur du grid l'autorise.
 - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application client S3 pour ajouter des objets et définir éventuellement la conservation propre à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si l'administrateur du grid l'autorise.
 - Conserver la date de fin : doit être inférieur ou égal à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API

REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors du téléchargement.

- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. Entrée d'objet

Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

- Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment par défaut sont ignorés.
- Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
- Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par le verrouillage objet S3.

Si les paramètres de conservation sont appliqués, l'objet et les métadonnées S3 définies par l'utilisateur sont protégés.

2. Conservation et suppression d'objets

StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité dans les politiques ILM actives. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

- Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Est-il toujours possible de gérer des compartiments existants conformes ?

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour obtenir des instructions, reportez-vous à la section

"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5".

Informations associées

Apprenez-en plus sur ["Exigences de verrouillage d'objet S3"](#)

Mettre à jour la rétention par défaut du verrouillage d'objet S3 dans StorageGRID

Si vous avez activé le verrouillage objet S3 lors de la création du compartiment, vous pouvez modifier ce dernier pour modifier les paramètres de conservation par défaut. Vous pouvez activer (ou désactiver) la rétention par défaut et définir un mode de rétention et une période de rétention par défaut.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Le verrouillage des objets S3 est activé globalement pour votre système StorageGRID et vous avez activé le verrouillage des objets S3 lorsque vous avez créé le compartiment. Voir ["Utilisez le verrouillage d'objet S3 pour conserver les objets"](#).

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **S3 Object Lock**.
4. En option, activez ou désactivez **rétention par défaut** pour ce compartiment.

Les modifications de ce paramètre ne s'appliquent pas aux objets qui se trouvent déjà dans le compartiment ni aux objets qui peuvent avoir leurs propres périodes de conservation.

5. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La gouvernance	• Les utilisateurs disposant de l'`s3:BypassGovernanceRetention` autorisation peuvent utiliser l'`x-amz-bypass-governance-retention: true` en-tête de la demande pour contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. Remarque : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

6. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le tenant, telle que définie par l'administrateur de la grille.

Une période de rétention *maximum*, qui peut être de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de rétention *default*, elle ne peut pas dépasser la valeur définie pour la période de rétention maximale. Si nécessaire, demandez à votre administrateur de grille d'augmenter ou de réduire la période de rétention maximale.

7. Sélectionnez **Enregistrer les modifications**.

Configurer CORS pour les compartiments S3 dans StorageGRID

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Pour les demandes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui a le ["Autorisation gérer tous les compartiments ou Afficher tous les compartiments"](#). Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui a le ["Autorisations de gestion de tous les compartiments"](#). Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le ["Autorisation d'accès racine"](#) permet d'accéder à toutes les demandes de configuration CORS.

Description de la tâche

Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons, par exemple, que vous utilisez un compartiment S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour le `Images` compartiment, vous pouvez autoriser l'affichage des images de ce compartiment sur le site Web `http://www.example.com`.

Activer le CORS pour un godet

Étapes

1. Utilisez un éditeur de texte pour créer le fichier XML requis. Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Détails :
 - Permet à n'importe quel domaine d'envoyer des requêtes GET au compartiment
 - Autorise uniquement le `http://www.example.com` domaine à envoyer des requêtes GET, POST et DELETE
 - Tous les en-têtes de demande sont autorisés

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

Pour plus d'informations sur le XML de configuration CORS, reportez-vous à la section "[Documentation Amazon Web Services \(AWS\) : guide de l'utilisateur d'Amazon simple Storage Service](#)".

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
3. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.
4. Dans l'onglet **Bucket Access**, sélectionnez l'accordéon **Cross-Origin Resource Sharing (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le fichier XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Enregistrer les modifications**.

Modifier le paramètre CORS

Étapes

1. Mettez à jour le XML de configuration CORS dans la zone de texte ou sélectionnez **Effacer** pour recommencer.
2. Sélectionnez **Enregistrer les modifications**.

Désactiver le paramètre CORS

Étapes

1. Décochez la case **Activer CORS**.
2. Sélectionnez **Enregistrer les modifications**.

Informations associées

["Configurer StorageGRID CORS pour une interface de gestion"](#)

Supprimer des objets d'un compartiment StorageGRID S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer les objets d'une ou de plusieurs compartiments.

Considérations et exigences

Avant d'effectuer ces étapes, notez les points suivants :

- Lorsque vous supprimez les objets d'un compartiment, StorageGRID supprime définitivement tous les objets et toutes les versions d'objets de chaque compartiment sélectionné de tous les nœuds et sites de votre système StorageGRID. StorageGRID supprime également les métadonnées d'objet associées. Vous ne pourrez pas récupérer ces informations.
- La suppression de tous les objets d'un compartiment peut prendre plusieurs minutes, jours, voire semaines, en fonction du nombre d'objets, de copies d'objet et d'opérations simultanées.
- Si un compartiment a ["Verrouillage objet S3 activé"](#), il peut rester à l'état **Suppression d'objets : lecture seule** pendant *années*.



Un compartiment qui utilise le verrouillage d'objet S3 restera à l'état **Suppression d'objets : lecture seule** jusqu'à ce que la date de conservation soit atteinte pour tous les objets et que toutes les mises en suspens légales soient supprimées.

- Pendant la suppression des objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Une fois tous les objets supprimés, le compartiment reste à l'état en lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
 - Ramener le compartiment en mode écriture et le réutiliser pour de nouveaux objets
 - Supprimez le compartiment
 - Conservez le compartiment en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si la gestion des versions d'objet est activée dans un compartiment, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations de suppression d'objets dans un compartiment.
- Si la gestion des versions d'objet est activée dans un compartiment, l'opération de suppression d'objets ne supprime pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Voir les informations sur la suppression d'objets dans un compartiment dans ["Suppression d'objets avec version S3"](#).
- Si vous utilisez ["réplication entre plusieurs grilles"](#), notez ce qui suit :
 - L'utilisation de cette option ne supprime aucun objet du compartiment de l'autre grille.

- Si vous sélectionnez cette option pour le compartiment source, l'alerte **échec de réplication multigrille** est déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoute d'objets au compartiment de l'autre grille avant de supprimer tous les objets "[désactiver la réplication entre les grilles](#)" du compartiment.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

Menu actions

- a. Cochez la case correspondant à chaque compartiment dans lequel vous souhaitez supprimer des objets.
- b. Sélectionnez **actions > Supprimer les objets dans le compartiment**.

Page de détails

- a. Sélectionnez un nom de compartiment pour afficher ses détails.
- b. Sélectionnez **Supprimer les objets dans le compartiment**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails, entrez **Oui** et sélectionnez **OK**.
4. Attendez que l'opération de suppression commence.

Au bout de quelques minutes :

- Une bannière d'état jaune s'affiche sur la page de détails du compartiment. La barre de progression représente le pourcentage d'objets supprimés.
- **(lecture seule)** apparaît après le nom du compartiment sur la page de détails du compartiment.
- **(Suppression d'objets : lecture seule)** apparaît à côté du nom du compartiment sur la page compartiments.

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)

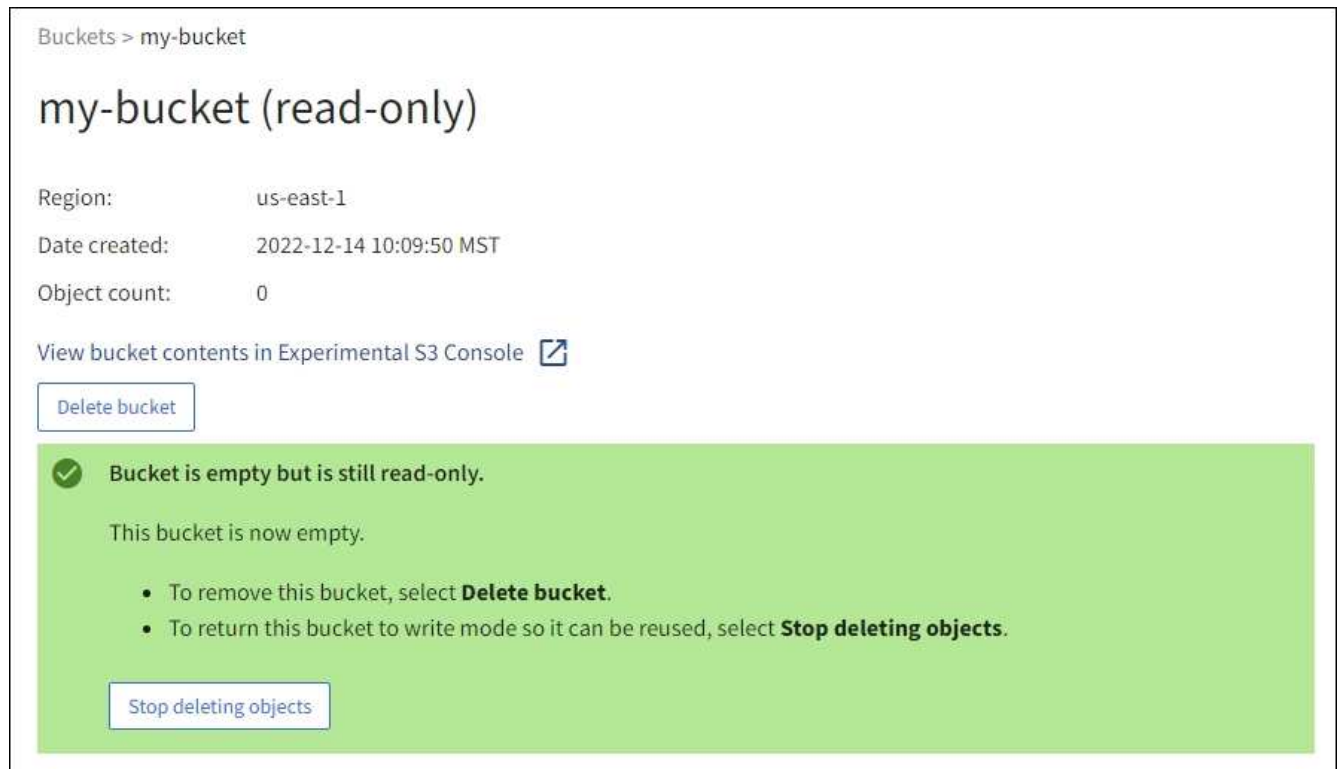
Stop deleting objects

5. Si nécessaire pendant l'exécution de l'opération, sélectionnez **Arrêter la suppression d'objets** pour arrêter le processus. Sélectionnez ensuite **Supprimer les objets dans le compartiment** pour reprendre le processus.

Lorsque vous sélectionnez **Arrêter la suppression d'objets**, le compartiment est remis en mode écriture ; cependant, vous ne pouvez pas accéder aux objets qui ont été supprimés ni les restaurer.

6. Attendez la fin de l'opération.

Lorsque le compartiment est vide, la bannière d'état est mise à jour, mais le compartiment reste en lecture seule.



7. Effectuez l'une des opérations suivantes :

- Quittez la page pour garder le compartiment en mode lecture seule. Par exemple, vous pouvez conserver un compartiment vide en mode lecture seule afin de réserver le nom du compartiment pour une utilisation ultérieure.
- Supprimer le compartiment. Vous pouvez sélectionner **Supprimer un compartiment** pour supprimer un seul compartiment ou retourner à la page compartiments et sélectionner **actions > Supprimer** compartiments pour supprimer plusieurs compartiments.



Si vous ne pouvez pas supprimer un compartiment multiversion après la suppression de tous les objets, les marqueurs de suppression peuvent rester. Pour supprimer le godet, vous devez supprimer tous les marqueurs de suppression restants.

- Ramenez le compartiment en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression d'objets** pour un seul compartiment ou revenir à la page compartiments et sélectionner **action > Arrêter la suppression d'objets** pour plusieurs compartiments.

Supprimer un compartiment StorageGRID S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer une ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Les compartiments à supprimer sont vides. Si les rubriques que vous souhaitez supprimer sont *not* vides,

["supprimez des objets du compartiment"](#).

Description de la tâche

Ces instructions expliquent comment supprimer un compartiment S3 à l'aide du Gestionnaire des locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de ["API de gestion des locataires"](#) ou de la ["L'API REST S3"](#).

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objets non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la suppression des objets avec version S3, reportez-vous à la section ["Comment supprimer les objets"](#).

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

Menu actions

- a. Cochez la case correspondant à chaque compartiment à supprimer.
- b. Sélectionnez **actions > Supprimer des compartiments**.

Page de détails

- a. Sélectionnez un nom de compartiment pour afficher ses détails.
- b. Sélectionnez **Supprimer le compartiment**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui**.

La fonction StorageGRID confirme que chaque compartiment est vide, puis supprime chaque compartiment. Cette opération peut prendre quelques minutes.

Si un compartiment n'est pas vide, un message d'erreur s'affiche. Vous devez ["supprimez tous les objets et tous les marqueurs de suppression dans le compartiment"](#) avant de pouvoir supprimer le compartiment.

Utilisez la console S3 dans StorageGRID

Vous pouvez utiliser la console S3 pour afficher et gérer les objets d'un compartiment S3.

Avec la console S3, vous pouvez :

- Télécharger, télécharger, renommer, copier, déplacer, et supprimer des objets
- Affichez, restaurez, téléchargez et supprimez des versions d'objet
- Recherche d'objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées d'objet
- Afficher, créer, renommer, copier, déplacer, et supprimez des dossiers

La console S3 améliore l'expérience utilisateur dans les cas les plus courants. Elle n'a pas été conçue pour remplacer les opérations de l'interface de ligne de commande ou de l'API dans tous les cas.



Si les opérations sont trop longues avec la console S3 (en minutes ou en heures, par exemple), tenez compte des points suivants :

- Réduction du nombre d'objets sélectionnés
- Accédez à vos données à l'aide de méthodes non graphiques (API ou interface de ligne de commande)

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires 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 racine. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation utiliser l'onglet de la console S3 et de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments. Voir ["Autorisations de gestion des locataires"](#).
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir ["Utilisez les règles d'accès au compartiment et au groupe"](#).
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Vous disposez éventuellement d'un `.csv` fichier contenant ces informations. Voir la ["instructions pour la création de clés d'accès"](#).

Étapes

1. Sélectionnez **Stockage > Compartiments > nom du compartiment**.
2. Sélectionnez l'onglet S3 Console.
3. Collez l'ID de clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Télécharger les clés d'accès** et sélectionnez votre `.csv` fichier.
4. Sélectionnez **connexion**.
5. Le tableau des objets de compartiment s'affiche. Vous pouvez gérer les objets selon vos besoins.

Informations supplémentaires

- **Recherche par préfixe** : la fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique par rapport au dossier en cours. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets dans les dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renvoie des objets se trouvant dans le `folder1/folder2/` dossier et commence par le mot `somefile-`.
- **Glisser-déposer** : vous pouvez faire glisser et 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 la gestion des versions de compartiment est désactivée** : lorsque vous écrasez ou supprimez un objet dans un compartiment avec la gestion des versions désactivée, l'opération est permanente. Voir ["Modifiez le contrôle de version d'objet pour un compartiment"](#).

Gérez les services de la plateforme S3

Services de plateforme S3

Découvrez les services de plateforme pour StorageGRID

Avant d'implémenter les services de plateforme, examinez la présentation et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, reportez-vous à ["UTILISEZ L'API REST S3"](#) la section .

Présentation des services de plateforme

Les services de plateforme StorageGRID vous aident à mettre en œuvre une stratégie de cloud hybride en vous permettant d'envoyer des notifications d'événements et des copies d'objets S3 et de métadonnées d'objet à des destinations externes.

L'emplacement cible des services de plateforme étant généralement externe à votre déploiement StorageGRID, les services de plateforme vous offrent la puissance et la flexibilité offertes par l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

Il est possible de configurer n'importe quelle combinaison de services de plateforme pour un seul compartiment S3. Par exemple, vous pouvez configurer à la fois ["Service CloudMirror"](#) et ["notifications"](#) sur un compartiment StorageGRID S3 afin de mettre en miroir des objets spécifiques vers Amazon Simple Storage Service (S3), tout en envoyant une notification concernant chaque objet à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.



L'utilisation des services de la plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Configuration des services de plate-forme

Les services de plateforme communiquent avec 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, un point de terminaison webhook ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un noeud final externe, vous pouvez activer un service de plate-forme pour un compartiment en ajoutant une configuration XML au compartiment. La configuration XML identifie les objets sur lesquels le compartiment doit agir, l'action que le compartiment doit effectuer et le point de terminaison que le compartiment doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plate-forme que vous souhaitez configurer. Par exemple :

- Si vous souhaitez que tous les objets dont les clés commencent par `/images` soient répliqués sur 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 compartiment, vous devez ajouter une configuration de notifications.
- Si vous souhaitez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification des métadonnées utilisée pour implémenter l'intégration de la recherche.

Le format du XML de configuration est régi par les API REST S3 utilisées pour mettre en œuvre les services

de plateforme StorageGRID :

Service de plateforme	L'API REST S3	Reportez-vous à la section
Réplication CloudMirror	• GetBuckeReplication • PutBuckeReplication	• "Réplication CloudMirror" • "Opérations sur les compartiments"
Notifications	• GetBucketNotifationConfiguration • PutBucketNotifationConfiguration	• "Notifications" • "Opérations sur les compartiments"
Intégration de la recherche	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plate-forme

Réflexion	Détails
Surveillance des terminaux de destination	Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.
Limitation du terminal de destination	Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination. Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer. Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Réflexion	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.
Suppressions d'objets basées sur des règles ILM	Pour correspondre au comportement de suppression des CRR AWS et Amazon simple notification Service, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours. Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.
À l'aide des terminaux Kafka	L'authentification des terminaux Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres terminaux, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe. • SASL/SIMPLE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Remarque : les paramètres du proxy de stockage configuré ne s'appliquent pas aux noeuds finaux des services de la plateforme Kafka.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Réflexion	Détails
État de la réplication	StorageGRID ne prend pas en charge la <code>x-amz-replication-status</code> barre de coupe.
Taille de l'objet	La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet <i>pris en charge</i>. Remarque : la taille <i>recommandée</i> maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

Réflexion	Détails
Gestion des versions du compartiment et ID de version	Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination. Lors de l'utilisation du versionnage, veuillez noter que l'ordre des versions d'objets dans le compartiment de destination est déterminé au mieux et n'est pas garanti par le service CloudMirror, en raison des limitations du protocole S3. De plus, les compartiments de destination conservent leurs propres paramètres et peuvent ne pas proposer de versionnage. Remarque : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.
Balisateur des versions d'objets	Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les objets normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.
Téléchargements partitionnés et ETag valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. Par conséquent, la ETag valeur de l'objet symétrique sera différente de celle ETag de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets cryptés avec SSE-C. si vous essayez d'ingérer un objet dans le compartiment source pour la réplication CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	Si le compartiment S3 source dans StorageGRID a S3 Object Lock activé, vous devez également activer S3 Object Lock pour le compartiment de destination avec la rétention par défaut configurée. La réplication des <i>données d'objet</i> est prise en charge pour les compartiments source et de destination avec S3 Object Lock activé. Toutefois, les compartiments de destination conserveront leurs propres paramètres de rétention des objets et peuvent ne pas proposer la conformité ou le versionnement.

Découvrez le service de réplication CloudMirror StorageGRID

Vous pouvez activer la réplication CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique les objets spécifiés ajoutés au compartiment vers un ou plusieurs compartiments de destination externes.

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



CloudMirror replication est prise en charge uniquement si le compartiment source a le verrouillage d'objet S3 activé et si le point de terminaison est un compartiment Amazon ou StorageGRID S3. Les paramètres de verrouillage d'objet ne sont pas répliqués vers le point de terminaison du compartiment.

CloudMirror et ILM

La réplication CloudMirror fonctionne indépendamment des règles ILM actives de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le compartiment source et les fournit au compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lors de la réussite de l'acquisition de l'objet.

CloudMirror et réplication intergrille

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Reportez-vous à la ["Comparez la réplication entre les grilles et la réplication CloudMirror"](#).

Compartiments CloudMirror et S3

La réplication CloudMirror est généralement configurée pour utiliser un compartiment S3 externe comme destination. Vous pouvez cependant également configurer la réplication afin d'utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Compartiments existants

Lorsque vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Les objets existants dans le compartiment ne sont pas répliqués. Pour forcer la réplication d'objets existants, vous pouvez mettre à jour les métadonnées de l'objet existant en effectuant une copie d'objet.



Si vous utilisez la réplication CloudMirror pour copier des objets vers une destination Amazon S3, sachez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de la requête PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Compartiments de destination multiples

Pour répliquer des objets d'un compartiment unique vers plusieurs compartiments de destination, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs compartiments en même temps.

Compartiments avec ou sans version

Vous pouvez configurer la réplication CloudMirror sur des compartiments avec ou sans version. Les compartiments de destination peuvent être avec ou sans version. Vous pouvez utiliser n'importe quelle combinaison de compartiments avec version et sans version. Par exemple, vous pouvez spécifier un compartiment avec version comme destination pour un compartiment source sans version, ou vice-versa. Vous pouvez également répliquer les compartiments sans version.

Suppression, boucles de réplication et événements

Comportement de suppression

Est identique au comportement de suppression du service Amazon S3, réplication interrégionale (CRR). La suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas versionné, la suppression d'un objet dans le compartiment source ne réplique pas le marqueur de suppression dans le compartiment de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

Comme les objets sont répliqués dans le compartiment de destination, StorageGRID les marque comme « répliqués ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliqués, ce qui vous protège contre les boucles de réplication accidentelles. Ce marquage de réplica est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lors de l'utilisation d'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 compartiment de destination

L'unicité et l'ordre des événements dans le compartiment de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

Découvrez les notifications d'événements StorageGRID pour les compartiments S3

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, à un point de terminaison webhook ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.

Les notifications d'événements sont créées au niveau du compartiment source, comme indiqué dans la configuration de la notification, et sont envoyées vers le compartiment de destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'événement peuvent être envoyées vers la destination après les opérations effectuées pour garantir la réussite de la livraison. La livraison étant asynchrone, l'ordre dans le temps des notifications au niveau de la destination n'est pas garanti correspondant à l'ordre des événements dans le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser la `sequencer` clé du message d'événement pour déterminer l'ordre des événements pour un objet spécifique, comme décrit dans la documentation Amazon S3.

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques restrictions.

- Les types d'événements suivants sont pris en charge :
 - s3:ObjectCreated :
 - s3:ObjectCreated:put
 - s3:ObjectCreated:Post
 - s3:ObjectCreated:Copier
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:objet Removed :
 - s3:ObjectRemoved:Supprimer
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post
- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	sgws:s3
Région de l'awsRegion	<i>non inclus</i>
x-amz-id-2	<i>non inclus</i>
arn	urn:sgws:s3:::bucket_name

Découvrez le service d'intégration de recherche StorageGRID

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

Le service d'intégration de la recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone des métadonnées d'objet S3 vers un terminal de destination lors de la création ou de la suppression d'un objet ou de la mise à jour de ses métadonnées ou de ses balises. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou de machine learning proposés par le service de destination pour rechercher, analyser et obtenir des informations exploitables à partir de vos données d'objet.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.

Même si l'intégration avec Elasticsearch peut être configurée dans un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation jusqu'à et l'état de conservation légale) des objets ne seront pas incluses dans les métadonnées envoyées à Elasticsearch.



Étant donné que le service d'intégration de recherche envoie des métadonnées d'objet à une destination, son XML de configuration est appelé « XML de configuration de notification_métadonnées_ ». Ce XML de configuration est différent du XML de configuration de notification utilisé pour activer les notifications *événement*.

Intégration de la recherche et compartiments S3

Vous pouvez activer le service d'intégration de la recherche pour tout compartiment avec version ou sans version. L'intégration des recherches est configurée en associant le XML de configuration des notifications de métadonnées au compartiment qui spécifie les objets à utiliser et la destination des métadonnées de l'objet.

Les notifications de métadonnées sont générées sous la forme d'un document JSON nommé avec le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant. Chaque notification de métadonnées contient un ensemble standard de métadonnées système pour l'objet, en plus de toutes les balises de l'objet et de toutes les métadonnées utilisateur.



Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Rechercher des notifications

Les notifications de métadonnées sont générées et mises en file d'attente pour être envoyées lorsque :

- Un objet est créé.
- Un objet est supprimé, notamment lorsque des objets sont supprimés suite au fonctionnement de la règle ILM de la grille.
- Les métadonnées ou les balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet de métadonnées et de balises est toujours envoyé lors de la mise à jour, et pas seulement les valeurs modifiées.

Après avoir ajouté le XML de configuration de notification des métadonnées à un compartiment, des notifications sont envoyées pour tout nouvel objet que vous créez et pour tout objet que vous modifiez en mettant à jour ses données, métadonnées utilisateur ou balises. Cependant, aucune notification n'est envoyée pour les objets qui se trouvaient déjà dans le compartiment. Pour vous assurer que les métadonnées d'objet de tous les objets du compartiment sont envoyées à la destination, effectuez l'une des opérations suivantes :

- Configurez le service d'intégration de la recherche immédiatement après avoir créé le compartiment et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà dans le compartiment pour déclencher un message de notification des métadonnées à envoyer à la destination.

Service d'intégration de la recherche et Elasticsearch

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch. Comme pour les autres services de plate-forme, la destination est spécifiée dans le noeud final dont l'URN est utilisé dans le XML de configuration du service. Utilisez le pour déterminer les "[Matrice d'interopérabilité NetApp](#)" versions de Elasticsearch prises en charge.

Gérez les terminaux des services de plateforme

Configurez les points de terminaison des services de plateforme dans StorageGRID

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison afin qu'il soit la destination du service de plateforme.

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 terminaux de services de plateforme. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plateforme ?

Un terminal 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 à partir d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un terminal des services de plateforme qui inclut les informations et les identifiants dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plate-forme nécessite son propre terminal, vous devez donc configurer au moins un point final pour chaque service de plate-forme que vous prévoyez d'utiliser. Après avoir défini un noeud final de services de plate-forme, vous utilisez l'URN du noeud final comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point final que la destination pour plusieurs compartiments source. Par exemple, vous pouvez configurer plusieurs compartiments source pour envoyer les métadonnées d'objet vers le même point de terminaison d'intégration de la recherche, afin d'effectuer des recherches dans plusieurs compartiments. Vous pouvez également configurer un compartiment source pour qu'il utilise plusieurs terminaux comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objets à une rubrique Amazon simple notification Service (Amazon SNS) et des notifications sur la suppression d'objets à une autre rubrique Amazon SNS.

Terminaux pour la réplication CloudMirror

StorageGRID prend en charge les terminaux de réplication qui représentent des compartiments S3. Ces compartiments peuvent être hébergés sur Amazon Web Services, sur le même déploiement StorageGRID, sur un autre service ou sur un autre déploiement à distance.

Terminaux pour les notifications

StorageGRID prend en charge les points de terminaison Amazon SNS, Kafka et webhook. Les points de terminaison Simple Queue Service (SQS) et AWS Lambda ne sont pas pris en charge.

Points d'extrémité du service d'intégration de la recherche

StorageGRID prend en charge des terminaux d'intégration de recherche représentant les clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un data Center local ou être hébergés dans un cloud AWS ou ailleurs.

Le point final de l'intégration de la recherche fait référence à un index et à un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant la création du noeud final dans StorageGRID, sinon la création du noeud final échouera. Il n'est pas nécessaire de créer le type avant de créer le noeud final. StorageGRID crée le type si nécessaire lors de l'envoi de métadonnées d'objet au terminal.

Informations associées

["Administrer StorageGRID"](#)

Spécifiez un URN pour un point de terminaison des services de plateforme StorageGRID

Lorsque vous créez un noeud final de services de plate-forme, vous devez spécifier un Nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le noeud final lorsque vous créerez un XML de configuration pour le service de plate-forme. L'URN de chaque terminal doit être unique.

StorageGRID valide les terminaux de services de plateforme lors de leur création. Avant de créer un noeud final de services de plate-forme, vérifiez que la ressource spécifiée dans le noeud final existe et qu'elle peut être atteinte.

Éléments DE RETOUR

L'URN d'un noeud final de services de plate-forme doit commencer par `urn:mysite` par `arn:aws`, 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 noeud final 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, kafka , ou webhook
Intégration de la recherche	es

Par exemple, pour continuer à spécifier l'URN d'un noeud final CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` à obtenir `urn:sgws:s3`.

Pour la plupart des points de terminaison, l'élément final de l'URN identifie la ressource cible spécifique à l'URI de destination, par exemple, `sns-topic-name`.

Pour les points de terminaison webhook, la ressource cible est l'URI de destination elle-même.

Service	Ressource spécifique
Réplication CloudMirror	bucket-name
Notifications	sns-topic-name OU kafka-topic-name Remarque : pour les points de terminaison webhook, l'élément final de l'URN peut être n'importe quelle chaîne, à condition que l'URN du point de terminaison soit unique.
Intégration de la recherche	domain-name/index-name/type-name Remarque : si le cluster Elasticsearch est NOT configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

Pour les entités AWS et GCP, l'URN complet est un ARN AWS valide. Par exemple :

- Réplication CloudMirror :

```
arn:aws:s3:::bucket-name
```

- Notifications :

```
arn:aws:sns:region:account-id:topic-name
```

- Intégration de la recherche :

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Pour un terminal d'intégration de recherche AWS, le domain-name doit inclure la chaîne littérale , `domain/` comme illustré ici.

Urnes pour des services hébergés localement

Lors de l'utilisation de services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute façon qui crée un URN valide et unique, tant que l'URN inclut les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués en blanc facultatif, ou vous pouvez les spécifier de quelque manière que ce soit pour vous aider à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :


```
urn:mysite:s3::bucket-name
```

Pour un noeud final CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide commençant par `urn:sgws:`:

```
urn:sgws:s3::bucket-name
```

- **Notifications :**

Spécifiez un point de terminaison Amazon simple notification Service :

```
urn:aws:sns:region:account-id:sns-topic-name
```

Spécifiez un terminal Kafka :

```
urn::kafka::kafka-topic-name
```



Vous pouvez également inclure `mysite` lors de la spécification d'un point de terminaison Kafka : `urn:mysite:kafka::kafka-topic-name`

Spécifiez un point de terminaison de webhook :

```
urn:mysite:webhook::webhook-name
```

- **Intégration de la recherche :**

```
urn:mysite:es::domain-name/index-name/type-name
```



Pour les noeuds finaux d'intégration de recherche hébergés localement, l'`domain-name`élément peut être n'importe quelle chaîne tant que l'URN du noeud final est unique.

Créer un point de terminaison de services de plateforme StorageGRID

Vous devez créer au moins un noeud final du type correct avant d'activer un service de plate-forme.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.

- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).
- La ressource référencée par le point de terminaison des services de la plateforme a été créée :
 - Réplication CloudMirror : compartiment S3
 - Notification d'événement : rubrique Amazon Simple Notification Service (Amazon SNS), rubrique Kafka ou point de terminaison webhook
 - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous disposez des informations relatives à la ressource de destination :
 - Hôte et port pour l'URI (Uniform Resource identifier)



Si vous prévoyez d'utiliser un compartiment hébergé sur un système StorageGRID comme point de terminaison pour la réplication CloudMirror, contactez l'administrateur de la grille pour déterminer les valeurs à saisir.

- Nom de ressource unique (URN)

["Spécifiez l'URN du terminal des services de plateforme"](#)

- Informations d'authentification (si nécessaire) :

Rechercher les terminaux d'intégration

Pour les terminaux 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

Terminaux de réplication CloudMirror

Pour les terminaux 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 (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.

Terminaux Amazon SNS

Pour les terminaux Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète

Les terminaux Kafka

Pour les terminaux Kafka, vous pouvez utiliser les identifiants suivants :

- 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 une vérification du certificat est requise)
- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des privilèges index and delete index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**. La page noeuds finaux des services de plate-forme s'affiche.
2. Sélectionnez **Créer un noeud final**.
3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

Le type de service de 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'identificateur de ressource unique (URI) du noeud final.

Utilisez l'un des formats suivants :

```
https://host:port
http://host:port
```

Si vous ne spécifiez pas de port, les ports par défaut suivants sont utilisés :

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des terminaux)
- Port 9092 pour les URI HTTPS et HTTP (terminaux Kafka uniquement)

Par exemple, l'URI d'un compartiment hébergé sur StorageGRID peut être :

```
https://s3.example.com:10443
```

Dans cet exemple, `s3.example.com` représente l'entrée DNS pour l'adresse IP virtuelle (VIP) du groupe haute disponibilité StorageGRID (HA), et `10443` représente le port défini dans le noeud final de l'équilibreur de charge.



Si possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge pour éviter un point de défaillance unique.

De la même manière, l'URI d'un compartiment hébergé sur AWS peut être :

```
https://s3-aws-region.amazonaws.com
```



Si le noeud final est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom de compartiment dans l'URI. Vous incluez le nom du compartiment dans le champ **URN**.

5. Entrez le nom de ressource unique (URN) du noeud final.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

6. Sélectionnez **Continuer**.

7. Sélectionnez une valeur pour **Type d'authentification**.



Si vous souhaitez une authentification pour les points de terminaison webhook, configurez Mutual Transport Layer Security (mTLS) dans [Étape 9](#).

Rechercher les terminaux d'intégration

Entrez ou téléchargez les informations d'identification d'un point final 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 terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Terminaux de réplication CloudMirror

Entrez ou téléchargez les informations d'identification d'un point final 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 terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

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 autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

Terminaux Amazon SNS

Saisissez ou téléchargez les informations d'identification d'un terminal 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 terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

Les terminaux Kafka

Entrez ou téléchargez les identifiants d'un terminal 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 terminaux dont la sécurité est désactivée.	Pas d'authentification.

Type d'authentification	Description	Informations d'identification
SASL/SIMPLE	Utilise un nom d'utilisateur et un mot de passe avec du 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 réponse de vérification 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 réponse de vérification et d'un hachage SHA-512 pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Sélectionnez **utiliser la délégation prise de l'authentification** si le nom d'utilisateur et le mot de passe proviennent d'un jeton de délégation obtenu à partir d'un cluster Kafka.

8. Sélectionnez **Continuer**.

9. Sélectionnez un bouton radio pour **Vérifier les certificats** pour choisir comment la connexion TLS au point de terminaison est vérifiée.

La plupart des points finaux

Vérifiez la connexion TLS pour l'intégration de la recherche, la réplication CloudMirror, Amazon SNS ou les points de terminaison Kafka.

Type de vérification du certificat	Description
TLS	Valide le certificat du serveur pour les connexions TLS à la ressource de point de terminaison.
Désactivées	La vérification du certificat est désactivée. Cette option n'est pas sécurisée.
Utiliser un certificat d'autorité de certification personnalisé	Le certificat CA personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison.
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.

Points de terminaison Webhook et Kafka

Vérifiez la connexion TLS pour les points de terminaison webhook ou Kafka.

Type de vérification du certificat	Description
TLS	Valide le certificat du serveur pour les connexions TLS à la ressource de point de terminaison.
mTLS	Valide les certificats client et serveur pour les connexions TLS mutuelles à la ressource de point de terminaison.
Désactivées	La vérification du certificat est désactivée. Cette option n'est pas sécurisée.
Utiliser un certificat d'autorité de certification personnalisé	Le certificat CA personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison.
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions. Remarque : Les points de terminaison Webhook ne disposent pas de cette option.

Lorsque vous sélectionnez **mTLS**, ces options deviennent disponibles.

Type de vérification du certificat	Description
Ne pas vérifier le certificat du serveur	Désactive la vérification du certificat du serveur, ce qui signifie que l'identité du serveur n'est pas vérifiée. Cette option n'est pas sécurisée.
Certificat client	Le certificat client est utilisé pour vérifier l'identité du client lors de la connexion au point de terminaison.
Clé privée du client	La clé privée du certificat client. S'il est chiffré, il doit utiliser le format traditionnel PKCS #1 (le format PKCS #8 n'est pas pris en charge).
Mot de passe de la clé privée du client	La phrase secrète permettant de décrypter la clé privée du client. Si la clé privée n'est pas chiffrée, laissez ce champ vide.

10. Sélectionnez **Test et Créer un noeud final**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Retour aux détails du noeud final** et mettez à jour les informations. Sélectionnez ensuite **Test et Créer un noeud final**.



La création du terminal échoue si les services de plate-forme ne sont pas activés pour votre compte de locataire. Veuillez contacter votre administrateur StorageGRID.

Après avoir configuré un noeud final, vous pouvez utiliser son URN pour configurer un service de plate-forme.

Informations associées

- ["Spécifiez l'URN du terminal des services de plateforme"](#)
- ["Configurez la réplication CloudMirror"](#)
- ["Configurer les notifications d'événements"](#)
- ["Configurez le service d'intégration de la recherche"](#)
- ["Ports utilisés pour les communications externes"](#)

Tester la connexion pour un point de terminaison des services de plateforme StorageGRID

Si la connexion à un service de plate-forme a changé, vous pouvez tester la connexion du noeud final pour vérifier que la ressource de destination existe et qu'elle peut être atteinte à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).

Description de la tâche

StorageGRID ne vérifie pas que les informations d'identification disposent des autorisations appropriées.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Sélectionnez le noeud final dont vous souhaitez tester la connexion.

La page des détails du point final s'affiche.

3. Sélectionnez **Tester la connexion**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Sélectionnez ensuite **Test et enregistrer les modifications**.

Modifier un point de terminaison de services de plateforme dans StorageGRID

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 les informations d'identification expirées ou modifier l'URI pour qu'il pointe vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un terminal de services de plateforme.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Sélectionnez le point final que vous souhaitez modifier.

La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.

4. Modifiez la configuration du noeud final selon les besoins.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

- a. Pour modifier le nom d'affichage du point de terminaison, sélectionnez l'icône de modification .
- b. Modifiez l'URI si nécessaire.

c. Si nécessaire, modifiez le type d'authentification.

- Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.
- Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.



La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non crypté.

d. Si nécessaire, modifiez la méthode de vérification des certificats.

5. Sélectionnez **Tester et enregistrer les modifications**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est vérifiée à partir d'un noeud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Modifiez le noeud final pour corriger l'erreur, puis sélectionnez **Test et enregistrer les modifications**.

Supprimer un point de terminaison des services de plateforme StorageGRID

Vous pouvez supprimer un noeud final si vous ne souhaitez plus utiliser le service de plate-forme associé.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Cochez la case correspondant à chaque point final à supprimer.



Si vous supprimez un noeud final de services de plate-forme en cours d'utilisation, le service de plate-forme associé sera désactivé pour tous les compartiments qui utilisent le noeud final. Toutes les demandes qui n'ont pas encore été traitées seront supprimées. Toutes les nouvelles demandes seront toujours générées jusqu'à ce que vous modifiiez la configuration de compartiment pour ne plus référencer l'URN supprimé. StorageGRID signale ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **actions > Supprimer le point final**.

Un message de confirmation s'affiche.

4. Sélectionnez **Supprimer le point final**.

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.

Déterminez si l'erreur s'est produite

Si des erreurs de noeud final de services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.

 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 s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des noeuds finaux, sélectionnez le noeud final qui contient l'erreur.
2. Sur la page de détails du point de terminaison, sélectionnez **Connection**. Cet onglet affiche uniquement l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps elle s'est produite. Les erreurs comportant l'icône X rouge  se sont produites au cours des 7 derniers jours.

Vérifiez si l'erreur est toujours à jour

Certaines erreurs peuvent continuer à s'afficher dans la colonne **dernière erreur**, même après leur résolution. Pour voir si une erreur est active ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez l'extrémité.

La page des détails du point final s'affiche.

2. Sélectionnez **connexion > Tester la connexion**.

La sélection de **Test Connection** permet à StorageGRID de valider l'existence du noeud final des services de plate-forme et de l'atteindre avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est "les informations d'identification du noeud final ou l'accès à la destination doivent être mis à jour" et les détails sont "AccessDenied" ou "InvalidAccessKeyId".

Si vous devez modifier le noeud final pour résoudre une erreur, la sélection de **Test et enregistrer les modifications** fait que StorageGRID valide le noeud final mis à jour et confirme qu'il peut être atteint avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez l'extrémité.
2. Sur la page des détails du noeud final, sélectionnez **Configuration**.
3. Modifiez la configuration de point final selon vos besoins.
4. Sélectionnez **connexion > Tester la connexion**.

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (tel que « 403 interdit »), vérifiez les autorisations associées aux informations d'identification du noeud final.

Informations associées

- ["Administration de StorageGRID ; dépannage des services de plate-forme"](#)
- ["Créer un terminal de services de plate-forme"](#)
- ["Tester la connexion pour le point final des services de plate-forme"](#)
- ["Modifier le point final des services de plate-forme"](#)

Configurez la réplication CloudMirror dans StorageGRID

Pour activer la réplication de CloudMirror pour un compartiment, vous créez et appliquez un XML de configuration de réplication de compartiment valide.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui servira de source de réplication.
- Le noeud final que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réplication CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal.

Pour des informations générales sur la réplication de compartiment et la configuration de celle-ci, reportez-vous à la section ["Documentation d'Amazon simple Storage Service \(S3\) : réplication d'objets"](#). Pour plus d'informations sur la manière dont StorageGRID implémente GetBuckeReplication, DeleteBuckeReplication et PutBuckeReplication, reportez-vous au ["Opérations sur les compartiments"](#).



La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir ["Comparez la réplication entre les grilles et la réplication CloudMirror"](#).

Notez les conditions et caractéristiques suivantes lors de la configuration de la réplication de CloudMirror :

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.
- La réplication est uniquement prise en charge pour les compartiments source ou de destination dont le verrouillage d'objet S3 est activé pour les compartiments Amazon S3 ou StorageGRID S3. Les en-têtes de verrouillage d'objet ne sont pas répliqués vers l'objet de destination.
- Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants du compartiment ne sont pas répliqués. Vous devez mettre à jour des objets existants pour déclencher la réplication.
- Si vous activez le verrouillage d'objet S3 sur le compartiment de destination après avoir configuré CloudMirror la réplication, vous devrez peut-être ["enregistrer à nouveau le point de terminaison"](#) pour autoriser la reprise de la réplication.
- Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :

- Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3.
- Lors de la configuration du XML :
 - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` l'élément pour les règles et respecte les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
 - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
 - Si vous le souhaitez, ajoutez l'élément et spécifiez l'une des options `<StorageClass>` suivantes :
 - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez un objet, la `STANDARD` classe de stockage est utilisée.
 - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données moins consultées, mais qui nécessitent 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 la `STANDARD` classe de stockage.
 - Si vous spécifiez un `Role` dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Replication**.

5. Cochez la case **Activer la réplication**.

6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que la réplication est configurée correctement :

- a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

Dans l'exemple présenté précédemment, les objets qui correspondent au préfixe « 2020 » sont répliqués.

- b. Confirmer que l'objet a été répliqué vers le compartiment de destination.

Pour les objets de petite taille, la réplication s'effectue rapidement.

Informations associées

["Créer un terminal de services de plate-forme"](#)

Configurez les notifications d'événements dans StorageGRID

Vous activez les notifications pour un compartiment en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un compartiment.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui sert de source de notifications.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour les notifications d'événements existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

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 Amazon SNS de destination, la rubrique Kafka ou le point de terminaison webhook spécifié comme URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, reportez-vous au ["Documentation Amazon"](#). Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous au ["Instructions d'implémentation des applications client S3"](#).

Notez les exigences et caractéristiques suivantes lors de la configuration des notifications d'événement pour un compartiment :

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un noeud final de notification d'événement pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un compartiment avec le verrouillage objet S3 activé, les métadonnées de verrouillage objet S3 (y compris la date de conservation jusqu'à et l'état 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, à la rubrique Kafka ou au point de terminaison webhook utilisé comme destination.
- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour le compartiment source :
 - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
 - Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.


```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) > seaux**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Event Notifications**.

5. Cochez la case **Activer les notifications d'événements**.

6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

- a. Exécutez une action sur un objet du compartiment source qui répond aux exigences de déclenchement d'une notification telles qu'elles sont configurées dans le fichier XML de configuration.

Dans cet 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 de destination, à la rubrique Kafka ou au point de terminaison du webhook.

Par exemple, si votre sujet de destination est hébergé sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est remise.

```

{
  "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 dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

- ["Description des notifications pour les compartiments"](#)
- ["UTILISEZ L'API REST S3"](#)

- ["Créer un terminal de services de plate-forme"](#)

Configurez le service d'intégration de recherche dans StorageGRID

Vous activez l'intégration de la recherche pour un compartiment en créant un XML d'intégration de recherche et en utilisant le Gestionnaire de locataires pour appliquer le XML au compartiment.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination.

Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Activer l'intégration de la recherche pour un compartiment :
 - 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 noeud final 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 les objets dont le préfixe est `images` donné à une destination, et des métadonnées pour les objets dont le préfixe est ajouté `videos` à une autre. Les configurations qui comportent des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisée.

Si nécessaire, reportez-vous à la [Exemples pour le XML de configuration des métadonnées](#).

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Éléments de la configuration de notification des métadonnées XML :

Nom	Description	Obligatoire
Configuration de la MetadaNotification Configuration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
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 d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'URNE est incluse dans l'élément destination.	Oui

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) > seaux**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Search Integration**

5. Cochez la case **Activer l'intégration de la recherche**.

6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de l'API Grid Manager ou de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :

- a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

Dans l'exemple présenté précédemment, tous les objets ajoutés au compartiment déclenchent une notification de métadonnées.

- b. Vérifiez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le noeud final.

Une fois que vous avez terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un compartiment à l'aide de l'une des méthodes suivantes :

- Sélectionnez **STORAGE (S3) > Buckets** et décochez la case **Enable search Integration**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

exemple : configuration de notification de métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Exemple : configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant au préfixe `/videos` sont envoyées à une seconde destination.

```

<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>

```

Format de notification des métadonnées

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé `SGWS/Tagging.txt` dans un compartiment nommé `test`. Le `test` compartiment n'est pas versionné, la balise est donc `versionId` 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 compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Informations sur les compartiments et les objets

bucket: Nom du compartiment

key: Nom de clé d'objet

versionID: Version de l'objet, pour les objets dans les compartiments multiversion

region: Région du compartiment, par exemple us-east-1

Métadonnées de système

size: Taille de l'objet (en octets) visible par un client HTTP

md5: Hachage d'objet

Métadonnées d'utilisateur

metadata: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur

key:value

Étiquettes

tags: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

key:value

Affichage des résultats dans Elasticsearch

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin

d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. 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 champ du document dans l'index.

UTILISEZ L'API REST S3

Versions et mises à jour prises en charge de l'API REST StorageGRID S3

StorageGRID prend en charge l'API simple Storage Service (S3), qui est implémentée en tant que ensemble de services web REST (Representational State Transfer).

La prise en charge de l'API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. L'utilisation actuelle des appels de l'API REST S3 par une application client requiert des modifications minimales.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de STS, S3 et HTTP :

Élément	Version
Spécification de l'API STS AssumeRole	"Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Assumerole" Pour plus d'informations sur AssumeRole, reportez-vous à "Configurer AssumeRole" .
Spécification de l'API S3	"Documentation AWS : Référence de l'API Amazon Simple Storage Service"
HTTP	1,1 Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). "IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)" Remarque: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Prise en charge des mises à jour de l'API REST S3

Relâchez	Commentaires
12.1.0	• <code>If-Match</code> L' <code>If-Match</code> en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut renvoyer un message d'erreur (501 Not Implemented). Si l' <code>If-Match</code> en-tête est accepté mais non fonctionnel, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict. • <code>If-None-Match</code> L' <code>If-None-Match</code> en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut entraîner un message d'erreur (501 Not Implemented). Si l' <code>If-None-Match</code> en-tête est accepté mais non fonctionnel, une alerte peut s'afficher avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict. • Ajout de la prise en charge des valeurs de somme de contrôle précalculées pour les requêtes et en-têtes suivants : ◦ <code>CompleteMultipartUpload</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, et <code>x-amz-checksum-crc64nvme</code> ◦ <code>CreateMultipartUpload</code>: <code>CRC32</code>, <code>CRC32C</code> et <code>CRC64NVME</code> pour <code>x-amz-checksum-algorithm</code> ◦ <code>CopyObject</code>: <code>CRC32</code>, <code>CRC32C</code>, <code>CRC64NVME</code>, et <code>SHA256</code> pour <code>x-amz-checksum-algorithm</code> ◦ <code>PutObject</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code> et <code>x-amz-checksum-crc64nvme</code> ◦ <code>UploadPart</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code> et <code>x-amz-checksum-crc64nvme</code> • Ajout de la prise en charge de <code>x-amz-checksum-type</code> pour <code>CreateMultipartUpload</code> et <code>CompleteMultipartUpload</code>. • Ajout de la prise en charge de la clé de condition de stratégie <code>s3:x-amz-copy-source</code>. • Autoriser l'activation du verrouillage d'objets S3 sur les compartiments existants.
12,0	• Ajout de la prise en charge du partage de ressources inter-origines (CORS) pour une interface de gestion, qui permet à un autre domaine d'accéder aux données dans StorageGRID à l'aide des API de gestion. "En savoir plus >>" . • Ajout de la prise en charge de STS AssumeRole et de la stratégie de session. Voir "un exemple de politique de session". Vous pouvez configurer AssumeRole dans les groupes de locataires.

Relâchez	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 pré-calculées pour les demandes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonction pour vérifier l'intégrité des objets téléchargés : ◦ Téléchargement CompleteMultipartUpload : x-amz-checksum-sha256 ◦ CreateMultipartUpload : x-amz-checksum-algorithm ◦ GetObject : x-amz-checksum-mode ◦ Objet principal : x-amz-checksum-mode ◦ ListParts ◦ PutObject : x-amz-checksum-sha256 ◦ UploadPart : x-amz-checksum-sha256 • Ajout de la possibilité pour l'administrateur du grid 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 compartiment et mode de conservation des objets : gouvernance ou conformité, si l'administrateur du grid l'autorise. ◦ La période de conservation par défaut du compartiment et la date de conservation de l'objet jusqu'au : doivent être inférieures ou égales à ce qui est autorisé par la période de conservation maximale définie par l'administrateur du grid. • Meilleure prise en charge de aws-chunked l'encodage de contenu et des valeurs de diffusion en continu x-amz-content-sha256. Limites : ◦ Le cas échéant, chunk-signature est facultatif et non validé ◦ S'il est présent, x-amz-trailer le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour qu'ils correspondent aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service" .
11,7	• Ajouté "Référence rapide : demandes d'API S3 prises en charge". • Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge de l'en-TÊTE de réponse spécifique à StorageGRID x-ntap-sg-cgr-replication-status pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grid. • Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.

Relâchez	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes GET Object et HEAD Object. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. • Ajout de la prise en charge de la <code>s3:object-lock-remaining-retention-days</code> clé de condition de règle pour définir la plage de périodes de conservation autorisées pour vos objets. • Modification de la taille <i>recommandée</i> maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
11,5	• Ajout de la prise en charge de la gestion du chiffrement de compartiment. • Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. • L' `Content-MD5` en-tête de la demande est désormais correctement pris en charge.
11,4	• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge. • Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. • Prise en charge supplémentaire des notifications de compartiment pour le <code>s3:ObjectRestore:Post</code> type d'événement. • Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Prise en charge supplémentaire des opérations de SUPPRESSION, d'OBTENTION et de MISE du cycle de vie du compartiment (action d'expiration uniquement) et de <code>x-amz-expiration</code> l'en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Relâchez	Commentaires
11,2	Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge. Remarque : les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.
11,0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout de la prise en charge des contraintes d'emplacement du balisage d'objets pour les compartiments, ainsi que de la cohérence disponible.
10,4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour la gestion des versions.
10,2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10,1	Ajout de la prise en charge du téléchargement en plusieurs parties, des requêtes de type hébergement virtuel et de l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID . La version actuellement prise en charge de la <i>Référence API du service de stockage simple</i> est 2006-03-01.

Requêtes S3 API prises en charge dans StorageGRID

Cette page explique comment StorageGRID prend en charge les API Amazon simple Storage Service (S3).

Cette page répertorie uniquement les opérations S3 prises en charge par StorageGRID. Toute opération S3 non répertoriée peut 501 Not Implemented ou entraîner un comportement inattendu.



Pour afficher la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf mention contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId` (comme requis pour les opérations d'objet)

Sauf mention contraire, les en-têtes de requête courants suivants sont pris en charge :

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations associées

- ["Détails de l'implémentation de l'API REST S3"](#)
- ["Référence de l'API Amazon simple Storage Service : en-têtes de demande communs"](#)

"AbortMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations pour les téléchargements partitionnés"](#)

"CompleteMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`

- x-amz-checksum-sha256
- x-amz-checksum-type
- x-amz-storage-class

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- ChecksumCRC32
- ChecksumCRC32C
- ChecksumCRC64NVME
- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentation StorageGRID

["CompleteMultipartUpload"](#)

"Objet de copie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- x-amz-checksum-algorithm
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

["Objet de copie"](#)

"CreateBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- x-amz-bucket-object-lock-enabled

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"CreateMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-checksum-type
- x-amz-server-side-encryption
- x-amz-storage-class

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

["CreateMultipartUpload"](#)

["DeleteBucket"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

["DeleteBuckeCors"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

["DeleteBuckeEncryption"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBuckeLifecycle"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

"DeleteBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus cet en-tête de demande supplémentaire :

- x-amz-bypass-governance-retention

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"DeleteObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus cet en-tête de demande supplémentaire :

- x-amz-bypass-governance-retention

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les objets"](#)

"DeleteObjectTagging"

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"GetBucketAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

"GetBucketLocation"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketNotificationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `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 demande supplémentaires :

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

Corps de la demande

Aucune

Documentation StorageGRID

["GetObject"](#)

["GetObjectAcl"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

["GetObjectLegalHold"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectLockConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"Godet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"Objet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande

Aucune

Documentation StorageGRID

["Objet principal"](#)

["Listseaux"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur le service et gt ; ListBuckets"](#)

["ListMultipartUploads"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres supplémentaires suivants :

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

Corps de la demande

Aucune

Documentation StorageGRID

["ListMultipartUploads"](#)

"ListObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres supplémentaires suivants :

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListObjectsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres supplémentaires suivants :

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres supplémentaires suivants :

- delimiter
- encoding-type

- key-marker
- max-keys
- prefix
- version-id-marker

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListParts"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres supplémentaires suivants :

- max-parts
- part-number-marker
- uploadId

Corps de la demande

Aucune

Documentation StorageGRID

["ListMultipartUploads"](#)

"PutBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- ApplyServerSideEncryptionByDefault

- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

"PutBucketNotifationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBuckePolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

Pour plus de détails sur les champs de corps JSON pris en charge, voir ["Utilisez les règles d'accès au compartiment et au groupe"](#) .

"PutBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Demander des balises XML de corps

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"Étiquetage PutBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBuckeVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Demander les paramètres du corps

StorageGRID prend en charge les paramètres de corps de demande suivants :

- VersioningConfiguration
- Status

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- 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 demande

- Données binaires de l'objet

Documentation StorageGRID

["PutObject"](#)

["PutObjectLegalHold"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#) ces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

["PutObjectLockConfiguration"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge la *plus grande partie* [paramètres et en-têtes communs](#) pour cette requête.

Corps de la demande

StorageGRID prend en charge la *plupart* des paramètres de corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation, à l'exception suivante :

Vous ne pouvez pas utiliser PutObjectLockConfiguration pour activer le verrouillage d'objet S3 sur un compartiment existant, sauf si votre administrateur de grille vous y a autorisé.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

["PutObjectRetention"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus l'en-tête supplémentaire suivant :

- `x-amz-bypass-governance-retention`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

"Marquage PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les objets"](#)

"Objet de restauration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous à la section ["Objet de restauration"](#).

"SelectObjectContent"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous aux sections suivantes :

- ["Utiliser S3 Select"](#)
- ["SelectObjectContent"](#)

"UploadPart"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `uploadId`

Et ces en-têtes de demande supplémentaires :

- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- 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 demande

- Données binaires de la pièce

Documentation StorageGRID

["UploadPart"](#)

["UploadPartCopy"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- uploadId

Et ces en-têtes de demande supplémentaires :

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corps de la demande

Aucune

Documentation StorageGRID

Tester la configuration de l'API REST S3 de StorageGRID

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services 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'interface de ligne de commande AWS à partir de ["aws.amazon.com/cli"](https://aws.amazon.com/cli/).
- Si vous le souhaitez ["créé un terminal d'équilibrage de charge"](#), vous avez . 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"](#).
- Vous avez ["Compte de locataire S3 créé"](#).
- Vous vous êtes connecté au locataire et ["créé une clé d'accès"](#) à .

Pour plus de détails sur ces étapes, reportez-vous ["Configurer les connexions client"](#) à la section .

Étapes

1. Configurez les paramètres de l'interface de ligne de commande AWS pour utiliser le compte que vous avez créé dans le système StorageGRID :
 - a. Entrer en mode de configuration : `aws configure`
 - b. Entrez l'ID de clé d'accès du compte que vous avez créé.
 - c. Entrez la clé d'accès secrète pour le compte que vous avez créé.
 - d. Entrez la région par défaut à utiliser. Par exemple `us-east-1`, .
 - e. Entrez le format de sortie par défaut à utiliser ou appuyez sur **entrée** pour sélectionner JSON.
2. Créer un compartiment.

Cet exemple suppose que vous avez configuré un noeud final d'équilibreur de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si le compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré dans l'exemple suivant :

```
"Location": "/testbucket"
```

3. Télécharger un objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si l'objet est téléchargé avec succès, un ETAG est renvoyé, qui est un hachage des données de l'objet.

4. Répertorier le contenu du compartiment pour vérifier que l'objet a été téléchargé.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
list-objects --bucket testbucket
```

5. Supprimez l'objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

6. Supprimer le compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

Implémentation de l'API REST S3 par StorageGRID

Comment l'API REST StorageGRID S3 résout les requêtes client conflictuelles

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ».

La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Comment l'API REST StorageGRID S3 équilibre la disponibilité et la cohérence

La cohérence assure un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs 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.

Si vous souhaitez effectuer des opérations d'objet de manière différente, vous pouvez :

- Spécifier une consistance pour [chaque godet](#) .
- Spécifiez une cohérence pour [Chaque opération d'API](#).
- Modifiez la cohérence par défaut à l'échelle de la grille en effectuant l'une des tâches suivantes :
 - Dans le gestionnaire de grille, accédez à **Configuration > Système > Paramètres de stockage > Cohérence du bucket 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` (recherchez **constencyLevel**).

Valeurs de cohérence

La cohérence affecte la manière dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds. La cohérence affecte la disponibilité des objets pour les demandes des clients.

Vous pouvez définir la cohérence d'une opération de compartiment ou d'API sur l'une des valeurs suivantes :

- **All** : tous les nœuds reçoivent immédiatement les métadonnées de l'objet ou la demande échoue.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites. Lorsque la sémantique du quorum est configurée, les comportements suivants s'appliquent :
 - Permet une tolérance aux pannes de site pour les demandes des clients lorsque les grilles comportent trois sites ou plus. Les réseaux à deux sites n'auront pas de tolérance aux pannes de site.
 - Les opérations S3 suivantes ne réussiront pas avec un site en panne :
 - DeleteBuckeEncryption
 - MettreBucketBranch
 - PutBucketEncryption
 - PutBuckeVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si nécessaire, vous pouvez ["configurer la sémantique du quorum StorageGRID pour une cohérence globale forte"](#) .

- **Strong-site** : les métadonnées de l'objet sont immédiatement distribuées à d'autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
- **Read-After-New-write** : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Utilisez la cohérence « lecture après nouvelle écriture » et « disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Read-after-New-write », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.
- Si cette recherche échoue, elle répète la recherche 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 « Read-after-New-write » mais que l'objet n'existe pas, la recherche d'objet atteint toujours une cohérence équivalente au comportement pour les opérations de type Strong-global. Cette cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles.

À moins que vous ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher 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 finale. Cette opération n'a pas abouti pour accroître la cohérence. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Indiquez la cohérence du fonctionnement de l'API

Pour définir la cohérence d'une opération d'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 « site fort » 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 compartiment, vous pouvez utiliser la requête StorageGRID ["PRÉSERVER la cohérence du godet"](#). Vous pouvez également ["modifier la cohérence d'un compartiment"](#) utiliser le Gestionnaire de locataires.

Lorsque vous définissez la cohérence d'un godet, tenez compte des points suivants :

- La cohérence d'un compartiment détermine la cohérence utilisée pour les opérations S3 exécutées sur les objets du compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- La cohérence d'une opération d'API individuelle remplace la cohérence du compartiment.
- En général, les compartiments doivent utiliser la cohérence par défaut, « Read-after-New-write ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet uniquement en dernier recours.

Comment les règles de cohérence et les règles ILM interagissent pour affecter la protection des données

La cohérence et les règles ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies d'objet. Comme StorageGRID requiert l'accès aux métadonnées et aux données d'un objet pour

répondre aux demandes des clients, le choix de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion permet une meilleure protection initiale des données et des réponses système plus prévisibles.

Les éléments suivants "options d'ingestion" sont disponibles pour les règles ILM :

Double allocation

StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie la réussite au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Stricte

Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que la réussite ne soit renvoyée au client.

Équilibré

StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée ; si cela n'est pas possible, des copies intermédiaires sont effectuées et le client est renvoyé avec succès. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Exemple d'interaction entre la règle de cohérence et la règle ILM

Supposons que vous ayez une grille à trois sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez trois copies d'objet, une sur le site local et une sur chaque site distant. Adoptez un comportement d'ingestion strict.
- **Cohérence** : Forte-globale (les métadonnées de l'objet sont immédiatement distribuées sur plusieurs sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les trois copies de l'objet et distribue les métadonnées à plusieurs sites avant de renvoyer l'opération 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 les sites distants. L'objet est entièrement récupérable sur les autres sites.

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 les sites distants, 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'inter-relation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Comment StorageGRID utilise le versionnage des objets

Vous pouvez définir l'état de gestion des versions d'un compartiment si vous souhaitez conserver plusieurs versions de chaque objet. L'activation de la gestion des versions pour un compartiment vous protège contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 10,000 versions de chaque

objet.

Le contrôle de version d'objets peut être associé à la gestion du cycle de vie des informations (ILM) d'StorageGRID ou à la configuration du cycle de vie des compartiments S3. Vous devez explicitement activer la gestion des versions pour chaque compartiment. Lorsque la gestion des versions est activée pour un compartiment, un ID de version est attribué à chaque objet ajouté au compartiment, qui est généré par le système StorageGRID.

La suppression de l'authentification multifacteur (MFA) n'est pas prise en charge.



Le contrôle de version ne peut être activé que pour les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les règles ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets, puis les évalue à nouveau en fonction de la règle ILM actuelle. Toute modification apportée aux règles ILM est appliquée à tous les objets précédemment ingérées. Ceci inclut les versions préalablement ingérées si la gestion des versions est activée. L'analyse ILM applique les modifications de l'ILM aux objets précédemment ingérées.

Pour les objets S3 dans les compartiments avec gestion des versions, la prise en charge de la gestion des versions vous permet de créer des règles ILM qui utilisent « Noncurrent Time » comme heure de référence (sélectionnez **Yes** pour la question « Apply this rule to Older object versions only? » ["Étape 1 de l'assistant de création de règles ILM"](#)(Appliquer cette règle aux versions d'objets plus anciennes uniquement ?) dans la section). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Noncurrent Time » vous permet de créer des stratégies 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 partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

Informations associées

- ["Suppression d'objets avec version S3"](#)
- ["Règles et règles ILM pour les objets avec version S3 \(exemple 4\)"](#).

Utilisez l'API REST S3 pour configurer StorageGRID S3 Object Lock

Si le paramètre global de verrouillage des objets S3 est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec le verrouillage des objets S3 activé. Vous pouvez spécifier des paramètres de conservation par défaut pour chaque compartiment ou pour chaque version d'objet.



StorageGRID ne prend pas en charge l'`x-amz-sdk-checksum-algorithm` en-tête de requête.

Activation du verrouillage objet S3 pour un compartiment

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, vous pouvez activer le verrouillage d'objet S3 lorsque vous créez chaque compartiment.

Le verrouillage objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3.

Pour activer le verrouillage d'objet S3 pour un compartiment, utilisez l'une de ces méthodes :

- Créez le compartiment à l'aide du Gestionnaire des locataires. Voir "[Créer un compartiment S3](#)".
- Créez le compartiment à l'aide d'une demande CreateBucket avec l'`x-amz-bucket-object-lock-enabled` en-tête de la demande. Voir "[Opérations sur les compartiments](#)".
- Gérez les paramètres du compartiment depuis le Gestionnaire de locataires. Voir "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".

Le verrouillage objet S3 requiert la gestion des versions des compartiments, qui est automatiquement activée lors de la création du compartiment. Vous ne pouvez pas suspendre la gestion des versions pour le compartiment. Voir "[Gestion des versions d'objet](#)".

Paramètres de conservation par défaut d'un compartiment

Lorsque le verrouillage objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la conservation par défaut du compartiment et spécifier un mode de conservation par défaut et une période de conservation par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
 - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
 - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
 - Les utilisateurs disposant de l'`s3:BypassGovernanceRetention` autorisation peuvent utiliser l'`x-amz-bypass-governance-retention: true` en-tête de la demande pour contourner les paramètres de rétention.
 - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Une période de conservation par défaut peut être spécifiée en années ou en jours pour chaque compartiment.

Comment définir la conservation par défaut d'un compartiment

Pour définir la rétention par défaut d'un compartiment, utilisez l'une des méthodes suivantes :

- Gérez les paramètres de compartiment depuis le gestionnaire de locataires. Voir "[Créer un compartiment S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".
- Exécutez une demande PutObjectLockConfiguration pour que le compartiment indique le mode par défaut et le nombre de jours ou d'années par défaut.

PutObjectLockConfiguration

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment pour lequel S3 Object Lock est activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

Lors de l'ingestion de nouvelles versions d'objets dans le compartiment, 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 rétention par défaut est utilisée pour calculer la date limite 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 fin de conservation de la version d'objet reste la même et n'est pas recalculée en fonction de la nouvelle période de conservation par défaut.

Vous devez disposer de l'`s3:PutBucketObjectLockConfiguration` autorisation, ou être root, pour effectuer cette opération.

Vous devez spécifier l'un des en-têtes de requête suivants dans la requête PutObjectLockConfiguration :

```
Content-MD5
x-amz-checksum-*
```



StorageGRID ne valide pas le contenu de l'en-tête `x-amz-checksum-*` pour cette opération.

Exemple de demande

Cet exemple active le verrouillage d'objet S3 pour un compartiment (si votre administrateur de grille a donné l'autorisation) et définit le mode de rétention par défaut sur COMPLIANCE et la période de rétention par défaut sur 6 ans.


```

PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>

```

Comment déterminer la conservation par défaut d'un compartiment

Pour déterminer si le verrouillage objet S3 est activé pour un compartiment et pour afficher le mode de conservation et la période de conservation par défaut, utilisez l'une des méthodes suivantes :

- Affichez le compartiment dans le gestionnaire de locataires. Voir ["Afficher les compartiments S3"](#).
- Émettre une demande `GetObjectLockConfiguration`.

GetObjectLockConfiguration

La demande `GetObjectLockConfiguration` vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, si ce dernier est activé, vérifiez s'il existe un mode de rétention et une période de rétention par défaut configurés pour le compartiment.

Lors de l'ingestion de nouvelles versions d'objets dans le compartiment, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de rétention par défaut est utilisée pour calculer la date limite de rétention si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Vous devez disposer de l'`s3:GetBucketObjectLockConfiguration` autorisation, ou être root, pour effectuer 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/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Comment spécifier les paramètres de conservation d'un objet

Un compartiment lorsque le verrouillage objet S3 est activé peut contenir une combinaison d'objets avec ou sans paramètres de conservation du verrouillage objet S3.

Les paramètres de conservation au niveau objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de conservation d'un objet remplacent les paramètres de conservation par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : CONFORMITÉ ou GOUVERNANCE.
- **Conserver-jusqu'à-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.
 - En mode CONFORMITÉ, si la date de conservation jusqu'à est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation jusqu'à peut être augmentée,

mais cette date ne peut pas être réduite ou supprimée.

- En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre conserver jusqu'à la date. Ils peuvent supprimer une version d'objet avant la fin de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation jusqu'à.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée.

Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date de conservation jusqu'à. Si une version d'objet est en attente légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet à un compartiment, émettez une **"PutObject"**, **"Objet de copie"** ou **"CreateMultipartUpload"** une demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, Qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).



Si vous spécifiez `x-amz-object-lock-mode`, vous devez également spécifier `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - La date de conservation doit être ultérieure.
- `x-amz-object-lock-legal-hold`

Si la conservation légale est ACTIVÉE (sensible à la casse), l'objet est placé sous une obligation légale. Si la mise en attente légale est désactivée, aucune mise en attente légale n'est mise. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de demande, tenez compte des restrictions suivantes :

- Vous devez inclure l'un des en-têtes de requête suivants si un en-tête de requête `x-amz-object-lock-*` est présent dans la requête PutObject :

```
Content-MD5
x-amz-checksum-*
```

Ces en-têtes ne sont pas requis pour CopyObject ou CreateMultipartUpload.

- Si le compartiment n'a pas le verrouillage d'objet S3 activé et qu'un en-tête de requête `x-amz-object-lock-*` 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 faire correspondre le comportement AWS. Cependant, lors de l'ingestion d'un objet dans un compartiment lorsque le verrouillage objet S3 est activé, StorageGRID effectue toujours une entrée à double validation.

- Une réponse ultérieure à la version GET ou HeadObject inclura les en-têtes `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` et `x-amz-object-lock-legal-hold`, s'il est configuré et si l'expéditeur de la demande a les autorisations correctes `s3:Get*`.

Vous pouvez utiliser la `s3:object-lock-remaining-retention-days` clé de condition de règle pour limiter les périodes de conservation minimale et maximale autorisée pour vos objets.

Comment mettre à jour les paramètres de conservation d'un objet

Si vous devez mettre à jour les paramètres de conservation légale ou de conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- `PutObjectLegalHold`

Si la nouvelle valeur de conservation légale est ACTIVÉE, l'objet est placé sous une mise en attente légale. Si la valeur de retenue légale est OFF, la suspension légale est levée.

- `PutObjectRetention`

- La valeur du mode peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).
- La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
- Si une version d'objet possède une date de conservation existante, vous pouvez uniquement l'augmenter. La nouvelle valeur doit être future.

Vous devez spécifier l'un des en-têtes de requête suivants dans la requête :

```
Content-MD5
x-amz-checksum-*
```



StorageGRID ne valide pas le contenu de l'en-tête `x-amz-checksum-*` pour ces opérations.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs disposant de cette `s3:BypassGovernanceRetention` autorisation peuvent contourner les paramètres de rétention actifs d'un objet qui utilise le mode de GOUVERNANCE. Toutes les opérations de SUPPRESSION ou de `PutObjectRetention` doivent inclure l'``x-amz-bypass-governance-retention:true`` en-tête de la demande. Ces utilisateurs peuvent effectuer les opérations supplémentaires suivantes :

- Exécutez les opérations `DeleteObject` ou `DeleteObjects` pour supprimer une version d'objet avant que sa période de rétention ne soit écoulée.

Impossible de supprimer les objets qui sont en attente légale. La mise en attente légale doit être désactivée.

L'``x-amz-bypass-governance-retention`` en-tête n'a aucun effet sur les objets sans S3 Object Lock.

- Exécutez des opérations PutObjectRetention qui changent le mode d'une version d'objet de GOUVERNANCE à CONFORMITÉ avant que la période de conservation de l'objet ne soit écoulée.

Le passage du mode DE CONFORMITÉ À LA GOUVERNANCE n'est jamais autorisé.

- Exécutez les opérations PutObjectRetention pour augmenter, diminuer ou supprimer la période de rétention d'une version d'objet.

Informations associées

- ["Gestion des objets avec le verrouillage d'objets S3"](#)
- ["Utilisez le verrouillage d'objet S3 pour conserver les objets"](#)
- ["Guide de l'utilisateur d'Amazon simple Storage Service : verrouillage d'objets"](#)

Découvrez la configuration du cycle de vie S3 pour StorageGRID

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

L'exemple simple présenté dans cette section illustre comment une configuration de cycle de vie S3 peut contrôler la suppression (expiration) de certains objets dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour des détails complets sur la création de configurations de cycle de vie S3, voir ["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.

La configuration du cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (à une date spécifique ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à partir de l'ingestion de l'objet.
- NonactualVersionExexpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- État
- ID

Chaque objet respecte les paramètres de conservation du cycle de vie d'un compartiment S3 ou une règle ILM. Lorsqu'un cycle de vie d'un compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la règle 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 des compartiments utilisent les paramètres de conservation de la règle 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 règle ILM ne sont pas utilisés et les versions d'objet sont conservées indéfiniment. Voir ["Exemples de priorités pour le cycle de vie des compartiments S3 et les règles ILM"](#).

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, voir ["Fonctionnement de ILM tout au long de la vie d'un objet"](#).



La configuration du cycle de vie des compartiments avec des compartiments dont le verrouillage objet S3 est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes.

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Créer une configuration de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont une `key2` valeur de `tag2`. Le `Expiration` paramètre indique 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` paramètre indique que les objets correspondant au filtre expireront 100 jours après leur ingestion.



Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets correspondants expirera 50 jours après qu'ils ne soient plus à jour.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

Appliquez la configuration du cycle de vie au compartiment

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande `PutBucketLifecycleConfiguration`.

Cette requête applique la configuration de cycle de vie du fichier d'exemple aux objets d'un compartiment nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration de cycle de vie a été correctement appliquée au compartiment, exécutez une demande `GetBucketLifecycleConfiguration`. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Une réponse réussie répertorie la configuration de cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration de cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête `PutObject`, `HeadObject` ou `GetObject`. Si une règle s'applique, la réponse inclut un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.



Étant donné que le cycle de vie d'un compartiment remplace ILM, la `expiry-date` date affichée est la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir "[Méthode de détermination de la conservation des objets](#)".

Par exemple, cette requête `PutObject` a été émise le 22 juin 2020 et place un objet dans le `testbucket` compartiment.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse de réussite indique que l'objet expirera dans 100 jours (01 oct 2020) et qu'il correspond à la règle 2 de la configuration de cycle de vie.


```
{
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\", rule-
id=\\"rule2\\",
  ETag: "\\"9762f8a803bc34f5340579d4446076f7\\""}
}
```

Par exemple, cette requête `HeadObject` a été utilisée pour obtenir les métadonnées du même objet dans le compartiment `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 compartiments avec gestion des versions, l'`x-amz-expiration` en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour la mise en œuvre de l'API REST S3 avec StorageGRID

Suivez ces recommandations lors de l'implémentation de l'API REST S3 pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser l'option « Disponible ». ["la cohérence"](#) . Par exemple, vous devez utiliser la cohérence « Disponible » si votre application HEAD un emplacement avant d'y effectuer un PUT.

Si non, si l'opération HEAD ne trouve pas l'objet, vous risquez de recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « disponible » pour chaque compartiment à l'aide de la ["PRÉSERVER la](#)

[cohérence du godel](#)" requête ou spécifier la cohérence dans l'en-tête de demande pour une opération d'API individuelle.

Recommandations pour les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction de la date de création du compartiment.

Compartiments créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez les recommandations d'AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, préfixez les clés d'objet à l'aide d'un nom de répertoire. C'est-à-dire, utilisez le format suivant :

```
mybucket/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mybucket/f8e3-image3132.jpg
```

Compartiments créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour répondre aux bonnes pratiques de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clé d'objet.



À cela s'exception près un workload S3 qui supprime en continu tous les objets après une courte période de temps. Pour minimiser l'impact sur les performances de ce cas d'utilisation, il est possible de faire varier la première partie du nom de clé tous les mille objets avec une date comme la date. Supposons par exemple qu'un client S3 écrit généralement 2,000 objets/seconde et que la règle de cycle de vie ILM ou compartiment supprime tous les objets au bout de trois jours. Pour réduire l'impact sur les performances, vous pouvez nommer les clés comme suit : `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recommandations pour les « lectures de plage »

Si "[option globale pour compresser les objets stockés](#)" est activé, les applications client S3 doivent éviter d'effectuer des opérations `GetObject` qui spécifient une plage d'octets. 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 objet très volumineux 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 client peuvent être en attente.



Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Prise en charge de l'API REST Amazon S3

Opérations prises en charge et limitations de l'API REST S3 dans StorageGRID

Le système StorageGRID implémente l'API simple Storage Service (API version 2006-03-01) avec la prise en charge de la plupart des opérations et avec certaines limites. Vous devez connaître les détails d'implémentation lorsque vous intégrez des applications client de l'API REST S3.

Le système StorageGRID prend en charge à la fois les requêtes de type hébergement virtuel et les requêtes de type chemin.

Traitement de la date

L'implémentation StorageGRID de l'API REST S3 ne prend en charge que les formats de date HTTP valides.

Le système StorageGRID prend uniquement en charge les formats de date HTTP valides pour tous les en-têtes qui acceptent les valeurs de date. La partie heure de la date peut être spécifiée au format heure de Greenwich (GMT) ou au format heure coordonnée universelle (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez l'`x-amz-date` en-tête dans votre demande, il remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS version 4, l'`x-amz-date` en-tête doit être présent dans la demande signée car l'en-tête de date n'est pas pris en charge.

En-têtes de demande commune

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "[Référence de l'API Amazon simple Storage Service : en-têtes de demande communs](#)", à une exception près.

En-tête de demande	Mise en place
Autorisation	Prise en charge complète de la signature AWS version 2 Prise en charge de la signature AWS version 4, à l'exception des cas suivants : • Lorsque vous fournissez la valeur de somme de contrôle de charge utile réelle dans <code>x-amz-content-sha256</code>, la valeur est acceptée sans validation, comme si la valeur <code>UNSIGNED-PAYLOAD</code> avait été fournie pour l'en-tête. Lorsque vous fournissez une <code>x-amz-content-sha256</code> valeur d'en-tête qui implique le <code>aws-chunked STREAMING</code> (par exemple, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), les signatures des blocs ne sont pas vérifiées par rapport aux données des blocs.

En-têtes de réponse commune

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par l'API *simple Storage Service Reference*, à une exception près.

En-tête de réponse	Mise en place
<code>x-amz-id-2</code>	Non utilisé

Comment l'API REST StorageGRID S3 authentifie les requêtes

Le système StorageGRID prend en charge l'accès authentifié et anonyme aux objets à l'aide de l'API S3.

L'API S3 prend en charge la version 2 de Signature et la version 4 de Signature pour authentifier les requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre ID de clé d'accès et de votre clé secrète d'accès.

Le système StorageGRID prend en charge deux méthodes d'authentification : l'en-tête HTTP `Authorization` et l'utilisation des paramètres de requête.

Utilisez l'en-tête HTTP `Authorization`

L'en-tête HTTP `Authorization` est utilisé par toutes les opérations de l'API S3, à l'exception des requêtes anonymes lorsque cela est autorisé par la stratégie de compartiment. L'`Authorization` en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs avec l'URL présignée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir un accès limité tiers à une ressource.

Opérations de service prises en charge dans StorageGRID

Le système StorageGRID prend en charge les opérations suivantes sur ce service.

Fonctionnement	Mise en place
Listseaux (Anciennement appelé GET Service)	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande StorageGRID " DÉCOUVREZ l'utilisation du stockage " 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 d'accès de / et un paramètre de requête personnalisée (<code>?x-ntap-sg-usage</code>) ajouté.
OPTIONS /	Les applications client peuvent émettre <code>OPTIONS /</code> des requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibres de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Opérations sur les compartiments S3 et détails d'implémentation dans StorageGRID

Le système StorageGRID prend en charge un maximum de 20 000 compartiments pour chaque compte locataire S3.

Chaque grille peut contenir un maximum de 100,000 compartiments.

Si plusieurs locataires disposent chacun de jusqu'à 5 000 compartiments, chaque nœud de stockage de la grille doit avoir un minimum de 64 Go de RAM.

Les restrictions relatives aux noms de compartiments suivent les restrictions de la région standard AWS US, mais vous devez les restreindre davantage aux conventions de nommage DNS pour prendre en charge les requêtes de type virtual-hosted-style S3.

Pour plus d'informations, veuillez consulter les documents suivants :

- ["Guide de l'utilisateur d'Amazon simple Storage Service : quotas de compartiments, restrictions et limites"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)

Les opérations ListObjects (GET Bucket) et ListObjectVersions (versions d'objet GET Bucket) prennent en charge StorageGRID ["valeurs de cohérence"](#) .

Vous pouvez vérifier si la mise à jour du temps d'accès est activée ou désactivée pour chaque compartiment. Consultez ["HEURE du dernier accès au compartiment"](#).

Le tableau suivant décrit la façon dont StorageGRID implémente les opérations des compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les informations d'identification d'accès nécessaires doivent être fournies pour le compte.

Fonctionnement	Mise en place
CreateBucket	Crée un nouveau compartiment. C'est en créant le compartiment que vous devenez le propriétaire. Remarque : Les compartiments de répertoire S3 ne sont pas pris en charge. - Les noms de compartiment doivent être conformes aux règles suivantes : - Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). - Doit être conforme DNS. - Doit contenir au moins 3 et 63 caractères. - Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. - Ne doit pas ressembler à une adresse IP au format texte. - Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. - Par défaut, les compartiments sont créés dans la <code>us-east-1</code> région ; vous pouvez cependant utiliser <code>LocationConstraint</code> l'élément de demande du corps de la demande pour spécifier une région différente. Lorsque vous utilisez l'élément <code>LocationConstraint</code>, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du Gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de région que vous devez utiliser. Remarque : Une erreur se produira si votre requête CreateBucket utilise une région qui n'a pas été définie dans StorageGRID. - Vous pouvez inclure l'en-tête de requête <code>x-amz-bucket-object-lock-enabled</code> pour créer un compartiment avec S3 Object Lock activé. Reportez-vous à "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". Le verrouillage d'objets S3 nécessite le versionnage des compartiments, qui est activé automatiquement lorsque vous créez le compartiment avec le verrouillage d'objets S3 activé. Vous pouvez activer le verrouillage des objets S3 lors de la création du compartiment ou à un moment ultérieur.
DeleteBucket	Supprime le godet.
DeleteBucketCors	Supprime la configuration CORS pour le godet.
DeleteBucketEncryption	Supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.

Fonctionnement	Mise en place
DeleteBucketLifecycle	Supprime la configuration du cycle de vie du compartiment. Reportez-vous à "Création de la configuration du cycle de vie S3" .
DeleteBucketPolicy	Supprime la règle associée au compartiment.
DeleteBucketReplication	Supprime la configuration de réplication attachée au compartiment.
DeleteBucketTagging	Utilise la <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un compartiment. Attention : Si une balise de stratégie ILM non standard est définie pour ce compartiment, il y aura une balise de compartiment <code>NTAP-SG-ILM-BUCKET-TAG</code> avec une valeur qui lui est attribuée. N'émettez pas de requête <code>DeleteBucketTagging</code> s'il existe une balise de compartiment <code>NTAP-SG-ILM-BUCKET-TAG</code>. Émettez plutôt une requête <code>PutBucketTagging</code> contenant uniquement la balise <code>NTAP-SG-ILM-BUCKET-TAG</code> et sa valeur attribuée pour supprimer toutes les autres balises du compartiment. Ne modifiez pas et ne supprimez pas la balise de compartiment <code>NTAP-SG-ILM-BUCKET-TAG</code>.
GetBucketAcl	Renvoie une réponse positive et l'ID, <code>DisplayName</code> et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
GetBucketCors	Renvoie la <code>cors</code> configuration du compartiment.
GetBucketEncryption	Renvoie la configuration de chiffrement par défaut du compartiment.
GetBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment GET)	Renvoie la configuration du cycle de vie du compartiment. Reportez-vous à "Création de la configuration du cycle de vie S3" .
GetBucketLocation	Renvoie la région qui a été définie à l'aide de l'élément <code>LocationConstraint</code> dans la requête <code>CreateBucket</code> . Si la région du compartiment est <code>us-east-1</code> (par défaut), une valeur vide est renvoyée pour <code>LocationConstraint</code> .
GetBucketNotificationConfiguration (Anciennement appelée notification GET Bucket)	Renvoie la configuration de notification associée au compartiment.
GetBucketPolicy	Renvoie la politique attachée au compartiment.

Fonctionnement	Mise en place
GetBuckeReplication	Renvoie la configuration de réplication attachée au compartiment.
GetBucketTagging	Utilise la <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un compartiment. Attention : Si une étiquette de stratégie ILM non standard est définie pour ce compartiment, il y aura une <code>NTAP-SG-ILM-BUCKET-TAG</code> étiquette de compartiment avec une valeur qui lui sera attribuée. Ne modifiez ni ne supprimez cette étiquette.
GetBucketVersioning	Cette implémentation utilise la <code>versioning</code> sous-ressource pour renvoyer l'état de gestion des versions d'un compartiment. • <i>Blank</i>: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
GetObjectLockConfiguration	Renvoie le mode de conservation par défaut du compartiment et la période de conservation par défaut, si elle est configurée. Consultez "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".
Godet principal	Détermine si un compartiment existe et que vous êtes autorisé à y accéder. Cette opération renvoie : • <code>x-ntap-sg-bucket-id</code>: UUID du compartiment au format UUID. • <code>x-ntap-sg-trace-id</code>: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
ListObjects et ListObjectsV2 (Anciennement appelé « GET Bucket »)	Renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un compartiment. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec l'`REDUCED_REDUNDANCY` option de classe de stockage : • STANDARD, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • GLACIER, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. Si le compartiment contient un grand nombre de clés supprimées dont le préfixe est identique, certains ne contiennent pas de <code>CommonPrefixes</code> clés. Pour les requêtes <code>HeadObject</code> et <code>ListObject</code>, <code>StorageGRID</code> renvoie les horodatages <code>LastModified</code> avec une précision différente tandis qu'AWS renvoie les horodatages avec la même précision, comme illustré dans les exemples suivants : • Objet principal <code>StorageGRID</code> : « LastModified » : « 2024-09-26T16:43:24+00:00 » • Objet de liste <code>StorageGRID</code> : « LastModified » : « 2024-09-26T16:43:24.931000+00:00 » • AWS <code>HeadObject</code> : « LastModified » : « 2023-10-17T00:19:54+00:00 » • AWS <code>ListObject</code> : « LastModified » : « 2023-10-17T00:19:54+00:00 »
ListObjectVersions (Anciennement nommé OBTENIR les versions de l'objet compartiment)	Avec l'accès EN LECTURE sur un compartiment, cette opération associée à la <code>versions</code> sous-ressource liste les métadonnées de toutes les versions des objets du compartiment.
PutBucketCors	Définit la configuration CORS pour un compartiment de sorte que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons, par exemple, que vous utilisez un compartiment S3 nommé <code>images</code> pour stocker des graphiques. En définissant la configuration CORS pour le <code>images</code> compartiment, vous pouvez autoriser l'affichage des images de ce compartiment sur le site Web <code>http://www.example.com</code>.

Fonctionnement	Mise en place
PutBucketEncryption	Définit l'état de chiffrement par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration du chiffrement côté serveur, définissez le <code>SSEAlgorithm</code> paramètre sur <code>AES256</code> et n'utilisez pas le <code>KMSMasterKeyID</code> paramètre. La configuration de chiffrement par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut l' `x-amz-server-side-encryption-*` en-tête de la requête).
PutBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment PUT)	Crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, Date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiation (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleteMultipartUpload • Transition Reportez-vous à "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action d'expiration dans le cycle de vie d'un compartiment interagit avec les instructions de placement ILM, reportez-vous à "Fonctionnement de ILM tout au long de la vie d'un objet". Remarque : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.

Fonctionnement	Mise en place
PutBucketNotificationConfiguration (Anciennement appelée notification PUT Bucket)	Configure les notifications pour le compartiment à l'aide du fichier XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants : • StorageGRID prend en charge les rubriques Amazon Simple Notification Service (Amazon SNS), les rubriques Kafka ou les points de terminaison webhook comme destinations. Les points de terminaison Simple Queue Service (SQS) ou AWS Lambda ne sont pas pris en charge. • La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, une 400 Bad Request erreur est renvoyée avec le code <code>InvalidArgument</code>. • Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements sont non pris en charge. ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante : ◦ EventSource <code>sgws:s3</code> ◦ AwsRegion non inclus ◦ x-amz-id-2 non inclus ◦ arn <code>urn:sgws:s3:::bucket_name</code>
PutBuckePolicy	Définit la politique associée au compartiment. Reportez-vous à "Utilisez les règles d'accès au compartiment et au groupe" .

Fonctionnement	Mise en place
PutBuckeReplication	Configure "Réplication StorageGRID CloudMirror" pour le compartiment à l'aide du fichier XML de configuration de réplication fourni dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID ne prend en charge que la V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de l'<code>Filter</code> élément pour les règles et suit les conventions de la V1 pour la suppression des versions d'objets. Pour plus de détails, consultez "Guide de l'utilisateur d'Amazon simple Storage Service : configuration de la réplication". • La réplication des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réplication. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés sous la forme de l'URN des points de terminaison StorageGRID, tels que définis dans le Tenant Manager ou l'API de gestion des locataires. Voir "Configurez la réplication CloudMirror". Le noeud final doit exister pour que la configuration de réplication réussisse. Si le noeud final n'existe pas, la demande échoue en tant que 400 Bad Request. le message d'erreur indique : Unable to save the replication policy. The specified endpoint URN does not exist: <code>URN</code>. • Vous n'avez pas besoin de spécifier un <code>Role</code> dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise la <code>STANDARD</code> classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le compartiment avant sa réplication, l'objet/le compartiment n'est pas répliqué et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réplication multi-région.

Fonctionnement	Mise en place
Étiquetage PutBucketTagging	Utilise la <code>tagging</code> sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse Attention : Si une balise de stratégie ILM non standard est définie pour ce compartiment, il y aura une balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment avec une valeur qui lui est attribuée. Assurez-vous que la balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment est incluse avec la valeur attribuée dans toutes les requêtes PutBucketTagging. Ne modifiez ni ne supprimez cette balise. Remarque : cette opération écrasera les balises actuelles du compartiment. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le compartiment.
PutBucketVersioning	Utilise la <code>versioning</code> sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes : • Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. • Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version <code>null</code>.
PutObjectLockConfiguration	• Configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut. • Si l'administrateur de la grille a donné son autorisation, active le verrouillage des objets S3 sur les compartiments existants. Si la période de conservation par défaut est modifiée, la date limite de conservation des versions d'objets existantes reste la même et n'est pas recalculée en fonction de la nouvelle période de conservation par défaut. Veuillez consulter "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour des informations détaillées.

Opérations sur les objets

Comment StorageGRID implémente les opérations de l'API REST S3 pour les objets

Cette section décrit la manière dont le système StorageGRID implémente les opérations

de l'API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations d'objet :

- StorageGRID "**valeurs de cohérence**" sont pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, y compris les objets créés par un utilisateur anonyme ou par un autre compte.

Le tableau ci-dessous décrit la manière dont StorageGRID implémente les opérations sur les objets de l'API REST S3.

Fonctionnement	Mise en place
DeleteObject	Lors du traitement d'une requête DeleteObject, 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 et indique que le client a réussi. Restrictions • L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge. • Les en-têtes <code>If-Match</code> et <code>If-None-Match</code> se comportent différemment selon la configuration de votre StorageGRID. Fournir ces en-têtes peut entraîner un message d'erreur (501 Not Implemented). Si les en-têtes <code>If-Match</code> ou <code>If-None-Match</code> sont acceptés mais non fonctionnels, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict. L' <code>x-amz-bypass-governance-retention</code> en-tête n'a aucun effet sur les objets sans S3 Object Lock. Gestion des versions Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la <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 à <code>true</code>. • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions activée, il génère un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression est renvoyé à l'aide de <code>x-amz-version-id</code> l'en-tête de réponse et l' <code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>. • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions suspendue, il entraîne la suppression permanente d'une version 'null' existante ou d'un marqueur de suppression 'null', et la génération d'un nouveau marqueur de suppression 'null'. L' <code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>. Remarque : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.

Fonctionnement	Mise en place
DeleteObjects (Précédemment nommé, SUPPRIMER plusieurs objets)	L'authentification multifacteur (MFA) et l'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. L'`x-amz-bypass-governance-retention` en-tête n'a aucun effet sur les objets sans S3 Object Lock. Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.
DeleteObjectTagging	Utilise la <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un objet. Gestion des versions Si le <code>versionId</code> 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 compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état <code>"MethodNotAllowed"</code> est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le <code>DisplayName</code> et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
GetObjectLegalHold	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
GetObjectRetention	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
GetObjectTagging	Utilise la <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un objet. Gestion des versions Si le <code>versionId</code> 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 compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état <code>"MethodNotAllowed"</code> est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
Objet principal	"Objet principal"

Fonctionnement	Mise en place
Objet de restauration	"Objet de restauration"
PutObject	"PutObject"
Objet de copie (Objet PUT précédemment nommé - Copier)	"Objet de copie"
PutObjectLegalHold	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
PutObjectRetention	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

Fonctionnement	Mise en place
Marquage PutObject	Utilise la <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 à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse Mises à jour des balises et comportement d'ingestion Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux. En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. Résolution des conflits Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération. Gestion des versions Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
SelectObjectContent	"SelectObjectContent"

Opérations Amazon S3 Select prises en charge dans StorageGRID

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le "Commande SelectObjectContent".



Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir ["SelectObjectContent"](#). Pour plus d'informations sur S3 Select, reportez-vous au ["Documentation AWS pour S3 Select"](#).

Seuls les comptes de tenant dont S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir la ["Considérations et configuration requise pour l'utilisation de S3 Select"](#).

Clauses

- SÉLECTIONNER la liste
- Clause FROM
- Clause WHERE
- Clause DE LIMITE

Types de données

- bool
- entier
- chaîne
- flottement
- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- < ;=
- >=
- =
- =
- <>
- !=
- ENTRE
- DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOY()
- NOMBRE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

Fonctions de conversion

- CAST (pour les types de données pris en charge)

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF
- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP

- CODE D'ARTICLE

Fonctions de chaîne

- CHAR_LENGTH, CARACTÈRE_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Comment StorageGRID utilise le chiffrement côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos objet. StorageGRID crypte les données lors de leur écriture et décrypte les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la gestion des clés de cryptage :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID crypte l'objet avec une clé unique. Lorsque vous émettez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour décrypter l'objet.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : lorsque vous émettez une demande S3 pour stocker un objet, vous fournissez votre propre clé de chiffrement. Lorsque vous récupérez un objet, vous fournissez la même clé de chiffrement dans le cadre de votre demande. Si les deux clés de chiffrement correspondent, l'objet est décrypté et vos données d'objet sont renvoyées.

StorageGRID gère toutes les opérations de cryptage et de décryptage des objets, mais vous devez gérer les clés de cryptage que vous fournissez.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, utilisez l'en-tête de demande suivant :

```
x-amz-server-side-encryption
```

L'en-tête de demande SSE est pris en charge par les opérations d'objet suivantes :

- "PutObject"
- "Objet de copie"
- "CreateMultipartUpload"

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de demande	Description
x-amz-server-side-encryption-customer-algorithm	Spécifiez l'algorithme de cryptage. La valeur de l'en-tête doit être AES256.
x-amz-server-side-encryption-customer-key	Spécifiez la clé de cryptage qui sera utilisée pour crypter ou décrypter l'objet. La valeur de la clé doit être codée en 256 bits, en base64.
x-amz-server-side-encryption-customer-key-MD5	Spécifiez le résumé MD5 de la clé de chiffrement selon la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du résumé MD5 doit être codée en base64 à 128 bits.

Les en-têtes de demande SSE-C sont pris en charge par les opérations objet suivantes :

- "GetObject"
- "Objet principal"
- "PutObject"
- "Objet de copie"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considérations relatives au chiffrement côté serveur avec clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des points suivants :

- Vous devez utiliser https.



StorageGRID rejette toute demande effectuée sur http lors de l'utilisation de SSE-C. pour des raisons de sécurité, vous devez considérer que toute clé que vous envoyez accidentellement à l'aide de http est compromise. Mettez la clé au rebut et tournez-la selon les besoins.

- L'ETag dans la réponse n'est pas le MD5 des données objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
- Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.
- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels que la rotation des clés, côté client.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication inter-grid ou CloudMirror est configurée pour le compartiment, vous ne pouvez pas acquérir d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

["Guide de l'utilisateur Amazon S3 : utilisation du chiffrement côté serveur avec des clés fournies par le client \(SSE-C\)"](#)

Créer une copie d'un objet dans StorageGRID avec la requête S3 CopyObject

Vous pouvez utiliser la requête CopyObject S3 pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject est identique à l'exécution de GetObject suivie de PutObject.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la ["téléchargement partitionné"](#) valeur.

La taille *supportée* maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).



Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus dans le nom ou la valeur de la clé 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 l'`x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé contient des caractères non imprimables.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- Content-Type
- x-amz-checksum-algorithm : Spécifiez CRC32, CRC32C, CRC64NVME, ou SHA256

Lorsque vous copiez un objet, si l'objet source possède un checksum ou inclut x-amz-checksum-algorithm, l'objet copié possède une somme de contrôle FULL_OBJECT.

Si l'objet source possède une somme de contrôle mais que la requête n'inclut pas x-amz-checksum-algorithm ou utilise une valeur de somme de contrôle non prise en charge, l'objet copié aura le même type de somme de contrôle que l'objet source. StorageGRID ignore les valeurs x-amz-checksum-algorithm invalides ou non prises en charge.

Si l'objet source ne possède pas de somme de contrôle et n'inclut pas x-amz-checksum-algorithm ou utilise une valeur de somme de contrôle non prise en charge, l'objet copié ne possède pas de somme de contrôle.



Si une requête CopyObject ne spécifie pas de somme de contrôle et que l'objet source n'en possède pas, StorageGRID ne calcule pas de somme de contrôle CRC-64/NVME par défaut pour un objet.

- 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 de REPLACE remplacer les métadonnées existantes lors de la copie de l'objet ou de 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 d'écraser les balises existantes lors de la copie de l'objet ou de mettre à jour les balises.

- En-têtes de demande de verrouillage d'objet S3 :
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#).

- En-têtes de demande SSE :
 - x-amz-copy-source-server-side-encryption-customer-algorithm
 - x-amz-copy-source-server-side-encryption-customer-key
 - x-amz-copy-source-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

Voir [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

L'`If-Match`-en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut renvoyer un message d'erreur (501 Not Implemented). Si l'`If-Match`-en-tête est accepté mais non fonctionnel, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- If-None-Match

L'`If-None-Match`-en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut entraîner un message d'erreur (501 Not Implemented). Si l'`If-None-Match`-en-tête est accepté mais non fonctionnel, une alerte peut s'afficher avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- x-amz-website-redirect-location

Options de classe de stockage

L'`x-amz-storage-class`-en-tête de requête est pris en charge et affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondante utilise la fonction Dual commit ou Balanced ["option d'ingestion"](#).

- STANDARD

(Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l'option `REDUCED_REDUNDANCY` est ignorée. Si vous ingérez un objet dans un compartiment compatible hérité, l'option `REDUCED_REDUNDANCY` renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Utilisation de `x-amz-copy-source` dans `CopyObject`

Si le compartiment source et la clé, spécifiés dans l'en-tête `x-amz-copy-source`, sont différents du compartiment et de la clé de destination, une copie des données de l'objet source est écrite vers la destination.

Si la source et la destination correspondent, et que l'en-tête `x-amz-metadata-directive` est spécifié comme `REPLACE`, les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la requête. Dans ce cas, StorageGRID ne réingère pas l'objet. Cela a deux conséquences importantes :

- Vous ne pouvez pas utiliser `CopyObject` pour chiffrer un objet existant ou pour modifier le chiffrement d'un objet existant. Si vous fournissez l'en-tête `x-amz-server-side-encryption` ou l'en-tête `x-amz-server-side-encryption-customer-algorithm`, StorageGRID rejette la demande et renvoie `XNotImplemented`.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toute modification du placement des objets déclenchée par la mise à jour est effectuée lorsque l'ILM est réévalué par les processus ILM d'arrière-plan normaux.

En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

Demander des en-têtes pour le cryptage côté serveur

Si vous ["utilisez le chiffrement côté serveur"](#), les en-têtes de requête que vous fournissez dépendent du cryptage de l'objet source et de l'intention de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la requête `CopyObject`, afin que l'objet puisse être décrypté puis copié :
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de 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 résumé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique que vous fournissez et gérez, incluez

les trois en-têtes suivants :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la nouvelle clé de chiffrement.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à ["utilisation du chiffrement 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 demande CopyObject :

- `x-amz-server-side-encryption`



La `server-side-encryption` valeur de l'objet ne peut pas être mise à jour. Au lieu de cela, faites une copie avec une nouvelle `server-side-encryption` valeur en utilisant `x-amz-metadata-directive: REPLACE`.

Gestion des versions

Si le compartiment source est versionné, vous pouvez utiliser l' `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 `versionId` sous-ressource. Si le compartiment de destination est versionné, la version générée est renvoyée dans l' `x-amz-version-id` en-tête de réponse. Si la gestion des versions est suspendue pour le compartiment cible, `x-amz-version-id` renvoie une valeur « null ».

Récupérer un objet depuis un bucket dans StorageGRID avec la requête GetObject

Vous pouvez utiliser la requête S3 GetObject pour récupérer un objet à partir d'un compartiment S3.

GetObject et objets multi pièces

Vous pouvez utiliser le `partNumber` paramètre request pour extraire une partie spécifique d'un objet multi pièce ou segmenté. L' `x-amz-mp-parts-count` élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir `partNumber` la valeur 1 pour les objets segmentés/multi pièces et les objets non segmentés/non multi pièces ; cependant, l' `x-amz-mp-parts-count` élément de réponse est renvoyé uniquement pour les objets segmentés ou multi pièces.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les requêtes GET pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas l' `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé contient des caractères non imprimables.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Accept-Encoding`

Lorsqu'un objet ne possède pas d' `Content-Encoding` stocké, une requête GET avec `Accept-Encoding: gzip` applique une compression à la volée à la réponse. Seul `gzip` affecte l'encodage de la réponse GET ; `deflate`, `br` et `identity` n'ont aucun effet. Pour les objets qui possèdent déjà un `Content-Encoding` stocké, `StorageGRID` renvoie l'encodage stocké et n'applique pas de compression supplémentaire à la volée en fonction de `Accept-Encoding`. `StorageGRID` ne prend pas en charge les opérations de lecture par plage pour les requêtes GET avec `Accept-Encoding: gzip`.

- `x-amz-checksum-mode`: Spécifiez `ENABLED`

L' `Range` en-tête n'est pas pris en charge `x-amz-checksum-mode` par 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 demande 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 aucune `versionId` sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "[Utilisez le cryptage côté serveur](#)".

Comportement de `GetObject` pour les objets de pool de stockage cloud

Si un objet a été stocké dans un "[Pool de stockage cloud](#)", le comportement d'une requête `GetObject` dépend de l'état de l'objet. Voir "[Objet principal](#)" 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 dans la grille, les requêtes GetObject tentent de récupérer les données de la grille avant de les extraire du pool de stockage cloud.

État de l'objet	Comportement de GetObject
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	200 OK Une copie de l'objet est récupérée.
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK Une copie de l'objet est récupérée.
L'objet a été transféré à un état non récupérable	403 Forbidden, InvalidObjectState Utilisez une " Objet de restauration " demande pour restaurer l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	403 Forbidden, InvalidObjectState Attendez la fin de la demande RestoreObject.
Objet entièrement restauré dans le pool de stockage cloud	200 OK Une copie de l'objet est récupérée.

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble de parties ou de 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 à 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 certaines données, mais s'arrête à mi-chemin du transfert.
- Une requête GetObject suivante peut renvoyer 403 Forbidden.

GetObject et la réplication inter-grille

Si vous utilisez "[fédération des grilles](#)" et "[réplication entre plusieurs grilles](#)" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GetObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• TERMINÉ : la réplication a réussi. • EN ATTENTE : l'objet n'a pas encore été répliqué. • ÉCHEC : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : l'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

Récupérer les métadonnées d'un objet dans StorageGRID avec la requête S3 HeadObject

Vous pouvez utiliser la requête S3 HeadObject pour extraire des métadonnées d'un objet sans renvoyer l'objet. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HeadObject pour déterminer l'état de transition de l'objet.

Objets en-tête et objets multi pièces

Vous pouvez utiliser `partNumber` le paramètre request pour extraire des métadonnées pour une partie spécifique d'un objet multi pièce ou segmenté. L' ``x-amz-mp-parts-count`` élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir `partNumber` la valeur 1 pour les objets segmentés/multi pièces et les objets non segmentés/non multi pièces ; cependant, l' ``x-amz-mp-parts-count`` élément de réponse est renvoyé uniquement pour les objets segmentés ou multi pièces.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les demandes HEAD pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas l' ``x-amz-missing-meta`` en-tête si le nom ou la valeur de la clé contient des caractères non imprimables.

En-tête de demande pris en charge

L'en-tête de demande suivant est pris en charge :

- `x-amz-checksum-mode`

Le `partNumber` paramètre et l' `Range`` en-tête 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 demande 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 aucune `versionId` sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section ["Utilisez le cryptage côté serveur"](#).

HeadObject Responses for Cloud Storage Pool objects

Si l'objet est stocké dans un ["Pool de stockage cloud"](#), les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet principal
Les objets sont ingérés dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	200 OK (Aucun en-tête de réponse spéciale n'est renvoyé.)

État de l'objet	Réponse à l'objet principal
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Jusqu'à ce que l'objet soit transféré à un état non récupérable, la valeur de <code>expiry-date</code> est définie sur un temps distant à l'avenir. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.
L'objet est passé à l'état non récupérable, mais il existe au moins une copie sur la grille	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" La valeur de <code>expiry-date</code> est définie sur un temps distant à l'avenir. Remarque : si la copie de la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre une "Objet de restauration" demande de restauration de la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet.
L'objet a été transféré à un état non récupérable et aucune copie n'existe sur la grille	200 OK x-amz-storage-class: GLACIER
Objet en cours de restauration à partir d'un état non récupérable	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"

État de l'objet	Réponse à l'objet principal
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 du pool de stockage cloud sera renvoyé à un état non récupérable.

Objets partitionnés ou segmentés dans Cloud Storage Pool

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête HeadObject peut être renvoyée de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été transférées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

HeadObject et réplication inter-grid

Si vous utilisez "fédération des grilles" et "réplication entre plusieurs grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête HeadObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• TERMINÉ : la réplication a réussi. • EN ATTENTE : l'objet n'a pas encore été répliqué. • ÉCHEC : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : l'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

Ajouter un objet à un compartiment dans StorageGRID avec la requête S3 PutObject

Vous pouvez utiliser la demande S3 PutObject pour ajouter un objet à un compartiment.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la "[téléchargement partitionné](#)" valeur.

La taille *supportée* maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).



Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête à 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans le codage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés 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 l'`x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé contient des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse

Propriété de l'objet

Dans StorageGRID, tous les objets sont détenus par le compte du propriétaire de compartiment, y compris les objets créés par un compte autre que le propriétaire ou un utilisateur anonyme.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- Cache-Control

- Content-Disposition
- Content-Encoding

Lorsque vous spécifiez `aws-chunked` pour Content-Encoding, StorageGRID ne vérifie pas les éléments suivants :

- StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données des blocs.
- StorageGRID ne vérifie pas la valeur que vous fournissez pour `x-amz-decoded-content-length` par rapport à l'objet.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

Le codage de transfert avec `chunked` est pris en charge si `aws-chunked` la signature de charge est également utilisée.

- En-têtes de requête de somme de contrôle :

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`



Si une requête `PutObject` ne spécifie pas de somme de contrôle, StorageGRID ne calcule pas de somme de contrôle CRC-64/NVME par défaut pour un objet.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur de `creation-time` est évaluée en secondes depuis le 1er janvier 1970.



Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et l'option d'acquisition équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de requête de verrouillage d'objet S3

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#).

- En-têtes de demande SSE :
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

Voir [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `If-Match`

L'`If-Match`-en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut renvoyer un message d'erreur (501 Not Implemented). Si l'`If-Match`-en-tête est accepté mais non fonctionnel, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- `If-None-Match`

L'`If-None-Match`-en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut entraîner un message d'erreur (501 Not Implemented). Si l'`If-None-Match`-en-tête est accepté mais non fonctionnel, une alerte peut s'afficher avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- `x-amz-acl`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`

- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

L'`x-amz-website-redirect-location` en-tête renvoie `XNotImplemented`.

Options de classe de stockage

L'`x-amz-storage-class` en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option strict d'ingestion, l' `x-amz-storage-class` en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- **STANDARD (Par défaut)**
 - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
 - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**
 - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
 - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. L' `REDUCED_REDUNDANCY` option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une copie répliquée unique. Dans ce cas, l'utilisation de `REDUCED_REDUNDANCY` supprime la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

L'utilisation de cette `REDUCED_REDUNDANCY` option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte des données d'objet lors de leur ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de

stockage qui échoue avant l'évaluation du ILM.



Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Le fait de spécifier `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lors de la première ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives, et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l'option `REDUCED_REDUNDANCY` est ignorée. Si vous ingérez un objet dans un compartiment compatible hérité, l'option `REDUCED_REDUNDANCY` renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE:** Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.

- `x-amz-server-side-encryption`

Lorsque l'en-tête `x-amz-server-side-encryption` n'est pas inclus dans la demande PutObject, la grille "[paramètre de chiffrement d'objet stocké](#)" est omise de la réponse PutObject.

- **SSE-C:** Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et gérez.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.

- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.

- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "[utilisation du chiffrement côté serveur](#)".



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Gestion des versions

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de

l' `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête autorisation

Lorsque vous utilisez l' `Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID ne nécessite pas l' `host` inclusion d'en-têtes dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas d' `Content-Type` être inclus dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas l' `x-amz-*` inclusion d'en-têtes dans `CanonicalHeaders`.



En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour vous assurer qu'ils sont vérifiés. Cependant, si vous excluez ces en-têtes, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, reportez-vous à ["Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile dans un seul bloc \(signature AWS version 4\)"](#) .

Informations associées

- ["Gestion des objets avec ILM"](#)
- ["Référence de l'API Amazon simple Storage Service : PutObject"](#)

Restaurez un objet dans StorageGRID avec la requête S3 RestoreObject

Vous pouvez utiliser la requête objet de restauration S3 pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID ne prend en charge que les requêtes `RestoreObject` pour restaurer un objet. Il ne prend pas en charge le `SELECT` type de restauration. Sélectionnez demandes retour `XNotImplemented`.

Gestion des versions

Si vous le souhaitez, spécifiez `versionId` pour restaurer une version spécifique d'un objet dans un compartiment multiversion. Si vous ne spécifiez pas `versionId` , la version la plus récente de l'objet est restaurée

Comportement de RestoreObject sur les objets de pool de stockage cloud

Si un objet a été stocké dans un ["Pool de stockage cloud"](#), une requête `RestoreObject` a le comportement suivant, en fonction de l'état de l'objet. Voir ["Objet principal"](#) 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 dans la grille, il n'est pas nécessaire de restaurer l'objet en émettant une requête `RestoreObject`. À la place, la copie locale peut être récupérée directement à l'aide d'une requête `GetObject`.

État de l'objet	Comportement de RestoreObject
L'objet est ingéré dans StorageGRID mais pas encore évalué par ILM ou l'objet ne se trouve pas dans un pool de stockage cloud	403 Forbidden, InvalidObjectState
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK Aucune modification n'est effectuée. Remarque : avant qu'un objet ne soit transféré à un état non récupérable, vous ne pouvez pas modifier son <code>expiry-date</code> .
L'objet a été transféré à un état non récupérable	202 Accepted Restaure une copie récupérable de l'objet vers le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la requête. À la fin de cette période, l'objet est renvoyé à un état non récupérable. Vous pouvez également utiliser <code>Tier</code> l'élément de demande pour déterminer la durée de la tâche de restauration pour terminer (<code>Expedited</code> , <code>Standard</code> ou <code>Bulk</code>). Si vous ne spécifiez pas <code>Tier</code> , le <code>Standard</code> niveau est utilisé. Important : Si un objet a été transféré vers S3 Glacier Deep Archive ou si le Cloud Storage Pool utilise Azure Blob Storage, vous ne pouvez pas le restaurer à l'aide du niveau <code>Expedited</code> . 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	409 Conflict, RestoreAlreadyInProgress
Objet entièrement restauré dans le pool de stockage cloud	200 OK Note : si un objet a été restauré à un état récupérable, vous pouvez le modifier <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.

Filtrer les données d'objets dans StorageGRID avec la requête S3 SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 à partir d'une instruction SQL simple.

Pour plus d'informations, voir ["Référence de l'API Amazon simple Storage Service : SelectObjectContent"](#).

Avant de commencer

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous disposez de l'autorisation pour l'objet que vous `s3:GetObject` souhaitez interroger.

- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet**. Exigences supplémentaires pour les objets parquet :
 - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets parquet.
 - S3 Select ne prend pas en charge la sortie parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
 - La taille maximale du groupe de lignes non compressées est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
 - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 MIB.

Exemple de syntaxe de demande CSV

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Exemple de syntaxe de demande de parquet

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Exemple de requête SQL

Cette requête obtient le nom de l'état, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

Les premières lignes du fichier à interroger, SUB-EST2020_ALL.csv, ressemblent 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, 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
```

Exemple d'utilisation de l'interface de ligne de commande AWS (parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

Les premières lignes du fichier de sortie, change.csv, se ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Opérations pour les téléchargements partitionnés

Opérations de chargement multiparties prises en charge dans StorageGRID

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement partitionné.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement partitionné :

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés vers un seul compartiment, car les résultats des requêtes ListMultipartUploads pour ce compartiment peuvent renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
 - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
 - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
 - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Chaque pièce étant considérée comme un objet unique, l'utilisation de pièces de grande taille réduit la surcharge liée aux métadonnées StorageGRID.
 - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- La gestion des règles ILM est évaluée pour chaque partie d'un objet en plusieurs parties lors de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé, si la règle ILM utilise la méthode équilibrée ou stricte "[option d'ingestion](#)". Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
 - Si des modifications sont apportées au ILM pendant un téléchargement partitionné S3, certaines

parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement partitionné terminé. Toute pièce qui n'est pas correctement placée est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.

- Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés sur DC1 alors que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque 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 partitionné, le ["Seuil de segmentation d'objet \(1 Gio\)"](#) n'est pas appliqué.
- Si nécessaire, vous pouvez l'utiliser ["chiffrement côté serveur"](#) avec les téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID), vous incluez l'en- `x-amz-server-side-encryption` tête de requête dans la requête CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec des clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de requête de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart suivante.
- Qu'un objet téléchargé en plusieurs parties soit inclus dans un ["seau de branche"](#) dépend de l'heure à laquelle l'ingestion a été initiée et du filtre temporel du compartiment de branche :
 - **Avant.** Si l'ingestion a été initiée avant l'horodatage *Before* du compartiment de branche, l'objet téléchargé en plusieurs parties est inclus, quelle que soit la date de fin du téléchargement.
 - **Après.** Si l'ingestion a été initiée après l'horodatage *After* du compartiment de branche, l'objet téléchargé en plusieurs parties est inclus.
 - **Entre.** Si l'ingestion a été initiée entre les horodatages *From* et *To* du compartiment de branche, l'objet téléchargé en plusieurs parties est inclus, quelle que soit la date et l'heure de fin du téléchargement.
 - **Exclude.** Si l'ingestion a été initiée avant l'heure *Exclude from* du compartiment de branche ou après l'heure *Exclude to*, l'objet téléchargé en plusieurs parties est inclus.

Fonctionnement	Mise en place
AbortMultipartUpload	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
CompleteMultipartUpload	Voir "CompleteMultipartUpload"
CreateMultipartUpload (Précédemment appelé lancer le téléchargement multipièce)	Voir "CreateMultipartUpload"
ListMultipartUploads	Voir "ListMultipartUploads"
ListParts	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Fonctionnement	Mise en place
UploadPart	Voir "UploadPart"
UploadPartCopy	Voir "UploadPartCopy"

Comment l'API REST S3 de StorageGRID effectue les chargements en plusieurs parties

L'opération CompleteMultipartUpload effectue un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.



StorageGRID prend en charge les valeurs non consécutives par ordre croissant pour le `partNumber` paramètre de requête avec CompleteMultipartUpload. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- En-têtes de requête de somme de contrôle :

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-checksum-type`



Si une requête CreateMultipartUpload ne spécifie pas de somme de contrôle, StorageGRID ne calcule pas de somme de contrôle CRC-64/NVME par défaut pour un objet.

- `x-amz-storage-class`

L'`x-amz-storage-class`en-tête affecte le nombre de copies objet créées par StorageGRID si la règle ILM correspondante spécifie le ["Double allocation ou option d'ingestion équilibrée"](#).

- STANDARD

(Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l'`REDUCED\_REDUNDANCY`option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l'`REDUCED\_REDUNDANCY`option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.



Si un téléchargement partitionné n'est pas terminé dans les 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.



La ETag 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 multipart.

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- If-Match

L'`If-Match`en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut renvoyer un message d'erreur (501 Not Implemented). Si l'`If-Match`en-tête est accepté mais non fonctionnel, une alerte peut être déclenchée avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- If-None-Match

L'`If-None-Match`en-tête se comporte différemment selon la configuration de votre StorageGRID. Fournir cet en-tête peut entraîner un message d'erreur (501 Not Implemented). Si l'`If-None-Match`en-tête est accepté mais non fonctionnel, une alerte peut s'afficher avec des instructions concernant l'activation du comportement d'erreur 501 Not Implemented plus strict.

- x-amz-checksum-md5
- x-amz-checksum-sha1
- x-amz-checksum-sha512
- x-amz-checksum-xxhash3
- x-amz-checksum-xxhash64
- x-amz-checksum-xxhash128

Gestion des versions

Cette opération termine un téléchargement partitionné. Si la gestion des versions est activée pour un compartiment, la version de l'objet est créée une fois le téléchargement partitionné terminé.

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de l'`x-amz-version-id`en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.



Lorsque le contrôle de version est activé pour un compartiment, le fait de terminer un téléchargement partitionné crée toujours une nouvelle version, même si des téléchargements partitionnés simultanés sont terminés sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un compartiment, il est possible de lancer un téléchargement partitionné et de lancer un autre lancement de téléchargement partitionné et de le terminer d'abord sur la même clé d'objet. Pour les compartiments non versionnés, le téléchargement partitionné de la dernière version est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel le téléchargement partitionné est configuré pour un service de plateforme, le téléchargement partitionné réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher la réplication ou la notification d'échec en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Reportez-vous à la ["Résoudre les problèmes liés aux services de plateforme"](#).

En-têtes et options des requêtes S3 CreateMultipartUpload dans StorageGRID

L'opération CreateMultipartUpload (précédemment appelée Initiate Multipart Upload) lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

L'`x-amz-storage-class` en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

Si la règle ILM correspondant à un objet ingéré utilise le paramètre strict ["option d'ingestion"](#), l'`x-amz-storage-class` en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- **STANDARD** (Par défaut)
 - **Dual commit** : si la règle ILM spécifie l'option d'acquisition Dual commit, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
 - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l'`x-amz-storage-class` en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

- **Dual commit** : si la règle ILM spécifie l'option Dual commit, StorageGRID crée une copie intermédiaire unique lorsque l'objet est ingéré (single commit).
- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. L' `REDUCED_REDUNDANCY` option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une copie répliquée unique. Dans ce cas, l'utilisation de `REDUCED_REDUNDANCY` supprime la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

L'utilisation de cette `REDUCED_REDUNDANCY` option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte des données d'objet lors de leur ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.



Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Le fait de spécifier `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lors de la première ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives, et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY` option est ignorée. Si vous ingérez un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-checksum-algorithm` : Spécifiez `CRC32`, `CRC32C`, `CRC64NVME`, ou `SHA256`



Si la requête `CreateMultipartUpload` ne spécifie pas de somme de contrôle, StorageGRID ne calcule pas de somme de contrôle `CRC-64/NVME` par défaut pour un objet. StorageGRID ignore les valeurs invalides ou non prises en charge `x-amz-checksum-algorithm`.

- `x-amz-checksum-type`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur de `creation-time` est évaluée en secondes depuis le 1er janvier 1970.



L'ajout de `creation-time` métadonnées définies par l'utilisateur n'est pas autorisé si vous ajoutez un objet à un compartiment pour lequel la conformité des données existantes est activée. Une erreur sera renvoyée.

- En-têtes de demande de verrouillage d'objet S3 :

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

- En-têtes de demande SSE :

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[Demander des en-têtes pour le cryptage côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID traite les caractères UTF-8, reportez-vous à la section ["PutObject"](#).

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de demande suivants pour crypter un objet partitionné avec un cryptage côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : utilisez l'en-tête suivant dans la demande `CreateMultipartUpload` si vous souhaitez crypter l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans les demandes `UploadPart`.
 - `x-amz-server-side-encryption`

- **SSE-C** : utilisez ces trois en-têtes dans la demande CreateMultipartUpload (et dans chaque demande UploadPart suivante) si vous souhaitez crypter l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "[utilisation du chiffrement côté serveur](#)".

En-têtes de requête non pris en charge

L'en-tête de demande suivant n'est pas pris en charge :

- `x-amz-website-redirect-location`

L'`x-amz-website-redirect-location` en-tête renvoie `\XNotImplemented`.

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est exécutée.

Fonctionnement S3 ListMultipartUploads et paramètres pris en charge dans StorageGRID

L'opération ListMultipartUploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération `CompleteMultipartUpload` est exécutée.

En-têtes de requête pris en charge et non pris en charge pour les opérations S3 UploadPart dans StorageGRID

L'opération `UploadPart` télécharge une pièce dans un téléchargement partitionné pour un objet.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- En-têtes de requête de somme de contrôle :

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`

Si vous avez spécifié une somme de contrôle CRC-32, CRC-32C, CRC-64/NVME ou SHA-256 lors de la requête `CreateMultipartUpload`, vous devez également inclure l'en-tête de requête de somme de contrôle dans chaque requête `UploadPart`.



Si une requête `CreateMultipartUpload` ne spécifie pas de somme de contrôle, StorageGRID ne calcule pas de somme de contrôle CRC-64/NVME par défaut pour un objet.

- `Content-Length`
- `Content-MD5`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour la demande `CreateMultipartUpload`, vous devez également inclure les en-têtes de requête suivants dans chaque demande `UploadPart` :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section ["Utilisez le cryptage côté serveur"](#).

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération `CompleteMultipartUpload` est exécutée.

Chargez une partie d'un objet dans StorageGRID avec l'opération S3 `UploadPartCopy`

L'opération `UploadPartCopy` télécharge une partie d'un objet en copiant les données d'un objet existant en tant que source de données.

L'opération `UploadPartCopy` est implémentée avec tout comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Cette requête lit et écrit les données d'objet spécifiées dans `x-amz-copy-source-range` au sein du système StorageGRID.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour la demande `CreateMultipartUpload`, vous devez également inclure les en-têtes de requête suivants dans chaque demande `UploadPartCopy` :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que

vous avez fournie dans la demande `CreateMultipartUpload`.

- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que celui que vous avez fourni dans la demande `CreateMultipartUpload`.

Si l'objet source est crypté 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 décrypté puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de 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 résumé MD5 que vous avez fourni lors de la création de l'objet source.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "[Utilisez le cryptage côté serveur](#)".

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération `CompleteMultipartUpload` est exécutée.

Prise en charge des sommes de contrôle S3

StorageGRID détecte automatiquement si une somme de contrôle a été spécifiée lors d'une requête `CreateMultipartUpload` et utilise cette somme de contrôle dans l'opération `UploadPartCopy`. Vous n'avez pas besoin de spécifier une somme de contrôle dans une requête `UploadPartCopy`. Si une requête `CreateMultipartUpload` ne spécifie pas de somme de contrôle, StorageGRID ne calcule pas de somme de contrôle CRC-64/NVME par défaut pour un objet. StorageGRID n'inclut pas de somme de contrôle pour la partie copiée lorsque `CreateMultipartUpload` n'a pas spécifié de somme de contrôle.

Réponses d'erreur de l'API REST StorageGRID S3

Le système StorageGRID prend en charge toutes les réponses d'erreur de l'API REST S3 standard qui s'appliquent. En outre, l'implémentation de StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
<code>AccessDenied</code>	403 interdit
<code>BadDigest</code>	400 demande erronée
<code>BucketAlreadyExists</code>	409 conflit

Nom	Statut HTTP
BucketNotEmpty	409 conflit
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAllowed	405 méthode non autorisée
MissingContentLength	411 longueur requise
Erreur MissingestBodyError	400 demande erronée

Nom	Statut HTTP
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d'implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée
UserKeyMustBeSpecified	400 demande erronée

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBuckeLifecycleNotAlldue	La configuration du cycle de vie des compartiments n'est pas autorisée dans un compartiment conforme aux anciennes	400 demande erronée
XBuckePolicyParseException	Impossible d'analyser la politique de compartiment JSON.	400 demande erronée
XComplianceConflitt	Opération refusée en raison des paramètres de conformité hérités.	403 interdit
XComplianceReduceRAIDForbidden	La réduction de la redondance est interdite dans le compartiment conforme aux réglementations existantes	400 demande erronée

Nom	Description	Statut HTTP
XMaxBucketPolicyLengthExcediédé	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée
XMissingInternalRequestHeader	En-tête d'une demande interne manquant.	400 demande erronée
XNoSuchBucketCompliance	La conformité héritée n'est pas activée dans le compartiment spécifié.	404 introuvable
XNotAcceptable	La demande contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 non acceptable
XNotImplementation	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non mis en œuvre

Opérations personnalisées StorageGRID

Opérations personnalisées de compartiment prises en charge dans 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.

Fonctionnement	Description
"OPTIMISEZ la cohérence des compartiments"	Renvoie la cohérence appliquée à un compartiment particulier.
"PRÉSERVER la cohérence du godet"	Définit la cohérence appliquée à un compartiment spécifique.
"HEURE du dernier accès au compartiment"	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.
"METTRE l'heure du dernier accès au compartiment"	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.
"SUPPRIMEZ la configuration de notification des métadonnées de compartiment"	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.

Fonctionnement	Description
"CONFIGURATION DES notifications de métadonnées de compartiment"	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.
"CONFIGURATION de notification des métadonnées de compartiment"	Configure le service de notification des métadonnées pour un compartiment.
"DÉCOUVREZ l'utilisation du stockage"	Indique la quantité totale de stockage utilisée par un compte et par compartiment associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.
"Obsolète : CONFORMITÉ DES compartiments"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.
"Obsolète : conformité DES compartiments PUT"	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.

Récupérez le niveau de cohérence du compartiment dans StorageGRID avec la requête GET Bucket consistency

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un compartiment spécifique.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBucketConsistency, ou être root de compte.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans le XML de réponse, <Consistency> renvoie l'une des valeurs suivantes :

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.

La cohérence	Description
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Exemple de réponse

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informations associées

["La cohérence"](#)

Spécifiez les niveaux de cohérence dans StorageGRID avec la requête PUT Bucket consistency

La demande de cohérence PUT Bucket vous permet d'indiquer la cohérence à appliquer aux opérations effectuées sur un compartiment.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckeConsistency, ou être root de compte.

Demande

Le `x-ntap-sg-consistency` paramètre doit contenir l'une des valeurs suivantes :

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Note: en général, vous devez utiliser la cohérence "lecture-après-nouvelle-écriture". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations associées

["La cohérence"](#)

Récupérez l'état de la dernière date d'accès au bucket dans StorageGRID avec la requête GET Bucket last access time

La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les compartiments individuels.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:GetBucketLastAccessTime`, ou être root de compte.

Exemple de demande

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre que les mises à jour du temps de dernier accès sont activées pour le compartiment.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Activer et désactiver les mises à jour du temps d'accès dans StorageGRID avec la requête PUT Bucket last access time

La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:PutBuckLastAccessTime` pour un compartiment ou être un compte root.



À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande PUT Bucket Last Access Time ou de la page de détails d'un compartiment dans le Gestionnaire de locataires. Voir "[Activez ou désactivez les mises à jour de l'heure du dernier accès](#)".

Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- Les requêtes `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 ne mettent à jour que les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le compartiment source, les requêtes `CopyObject` ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, les requêtes `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.
- `CompleteMultipartUpload` demande la mise à jour de l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple permet d'activer le temps du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Cet exemple désactive l'heure du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Désactivez le service d'intégration de recherche avec la requête **DELETE** Bucket metadata notification configuration dans StorageGRID

La demande de configuration DE notification DE métadonnées **DELETE** Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:DeleteBuceMeteatanotification` pour un compartiment, ou être un compte root.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un compartiment.


```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configurez l'intégration de la recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment 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 chaque compartiment.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:GetBucketMetadatanotification`, ou être root de compte.

Exemple de demande

Cette requête récupère la configuration de notification des métadonnées pour le compartiment nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

L'organe de réponse inclut la configuration de notification des métadonnées pour le compartiment. La configuration de notification des métadonnées vous permet de déterminer la configuration du compartiment pour l'intégration de la recherche. En d'autres termes, il vous permet de déterminer les objets à indexer et à quels terminaux leurs métadonnées d'objet sont envoyées.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle indique les objets qu'elle s'applique ainsi que la destination à laquelle StorageGRID doit envoyer les métadonnées d'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID.

Nom	Description	Obligatoire
Configuration de la MetadataNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui

Nom	Description	Obligatoire
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui

Exemple de réponse

Le XML inclus entre les

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` balises montre comment l'intégration avec un noeud final d'intégration de recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé `current` et 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-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

["Utilisez un compte de locataire"](#)

Activez le service d'intégration de recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment PUT

La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:PutBucketMetadanotification` pour un compartiment ou être un compte root.

Demande

La demande doit inclure la configuration de notification de métadonnées dans l'organisme de demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets à lesquels elle s'applique, ainsi que la destination vers laquelle StorageGRID doit envoyer les métadonnées d'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour les objets dont le préfixe est associé à une destination et pour `/images` les objets dont le préfixe est préfixe `/videos` à une autre.

Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe et une

seconde règle pour les objets avec test le préfixe test2 ne serait pas autorisée.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID. Le noeud final doit exister lorsque la configuration de notification des métadonnées est soumise, ou la demande échoue en tant que 400 Bad Request. le message d'erreur indique: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfig uration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui

Exemples de demandes

Cet exemple montre l'activation de l'intégration de la recherche pour un compartiment. Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Dans cet exemple, les métadonnées d'objet des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant au préfixe `/videos` sont envoyées à une seconde destination.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333: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 la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé `SGWS/Tagging.txt` dans un compartiment nommé `test`. Le `test` compartiment n'est pas versionné, la balise est donc `versionId` vide.


```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom de l'élément	Description
Informations sur les compartiments et les objets	godet	Nom du compartiment
Informations sur les compartiments et les objets	clé	Nom de clé d'objet
Informations sur les compartiments et les objets	ID de version	Version d'objet, pour les objets dans les compartiments multiversion
Informations sur les compartiments et les objets	région	Région de compartiment, par exemple <code>us-east-1</code>
Métadonnées de système	taille	Taille de l'objet (en octets) visible par un client HTTP
Métadonnées de système	md5	Hachage d'objets
Métadonnées d'utilisateur	métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur pour l'objet, comme paires de clé-valeur

Type	Nom de l'élément	Description
Étiquettes	balises <i>key:value</i>	Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur



Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Informations associées

["Utilisez un compte de locataire"](#)

Récupérez l'utilisation du stockage du compte et du bucket dans StorageGRID avec la requête GET Storage Usage

La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

La quantité de stockage utilisée par un compte et ses compartiments peut être obtenue par une demande ListBuckets modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage par compartiment est suivie séparément des demandes DE PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. S'il est impossible d'obtenir une cohérence globale élevée, StorageGRID tente de récupérer les informations relatives à l'utilisation de façon cohérente sur les sites.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:ListAllMyseaux` ou être root de compte.

Exemple de demande

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre un compte qui contient quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Gestion des versions

Chaque version d'objet stockée contribuera aux ObjectCount valeurs et DataBytes dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au ObjectCount total.

Informations associées

["La cohérence"](#)

Demandes de compartiment obsolètes pour la conformité des anciennes

Requêtes de compartiment obsolètes pour la conformité StorageGRID héritée

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

Fonction de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de compartiments avec la conformité activée. Toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les compartiments conformes existants.

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Gestion des objets avec ILM"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Obsolète - METTRE les modifications de la demande de godet à des fins de conformité"](#)

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

- ["Obsolète : OBTENEZ la conformité des compartiments"](#)

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

- ["Obsolète : conformité DES compartiments PUT"](#)

La demande DE conformité DE PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

Élément SGCompliance obsolète dans StorageGRID

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de requête XML facultatif des requêtes CreateBucket pour créer un compartiment compatible.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de compartiments avec la fonctionnalité conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de demande CreateBucket pour la conformité afin de créer un nouveau compartiment compatible :

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Requête GET Bucket de conformité obsolète dans StorageGRID

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#)

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:GetBucketCompliance` ou être root de compte.

Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité du compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans le XML de réponse, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525,600 minutes), à partir de l'ingestion de l'objet dans la grille. Il n'y a actuellement aucune retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après un an.

```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found, avec un code d'erreur S3 de XNoSuchBucketCompliance.

Requête PUT Bucket compliance obsolète dans StorageGRID

La demande DE conformité DE PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#)

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3:PutBucketCompliance`, ou être root de compte.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une demande de conformité PUT Bucket.

Exemple de demande

Cet exemple de demande modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront conservés pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de la date d'ingestion de l'objet dans la grille. Il n'y a pas de retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. Important lorsque vous spécifiez une nouvelle valeur pour <code>RetentionPeriodMinutes</code>, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.

Nom	Description
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence pour les paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 avec une demande DE conformité PUT bucket, StorageGRID tente de mettre à jour les métadonnées du compartiment dans la grille. Par défaut, StorageGRID utilise la cohérence **strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment disposent d'une cohérence de lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **strong-global** car un site de centre de données ou plusieurs nœuds de stockage sur un site sont indisponibles, le code d'état HTTP de la réponse est 503 Service Unavailable.

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur du grid ne parvient pas à rendre suffisamment de nœuds de stockage disponibles sur chaque site, le support technique peut vous demander de réessayer la demande en forçant la cohérence **strong-site**.



Ne forcez jamais la cohérence **Strong-site** pour la conformité PUT bucket à moins que vous n'ayez été dirigé pour le faire par le support technique et à moins que vous ne compreniez 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 en lecture après écriture uniquement pour les demandes des clients au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un compartiment dans une conservation légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation de la cohérence **strong-site**, relancez la demande de conformité PUT Bucket et incluez l' `Consistency-Control` en-tête de requête HTTP, comme suit :


```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found.
- Si `RetentionPeriodMinutes` dans la requête est inférieure à la période de conservation actuelle du compartiment, le code d'état HTTP est 400 Bad Request.

Informations associées

"Obsolète : [METTEZ les modifications de la demande de compartiment à des fins de conformité](#)"

Gérer les politiques d'accès

Comment StorageGRID utilise les politiques AWS pour contrôler l'accès aux compartiments et objets S3

StorageGRID utilise le langage de règles Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets dans ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de règles de l'API REST S3. Les règles d'accès de l'API S3 sont écrites au format JSON.

Présentation de la stratégie d'accès

StorageGRID prend en charge trois types de politiques d'accès :

- **Stratégies de compartiment**, gérées à l'aide des opérations de l'API `GetBucketPolicy`, `PutBucketPolicy` et `DeleteBucketPolicy` S3 ou du gestionnaire de locataires ou de l'API de gestion des locataires. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et peut-être plusieurs compartiments.
- **Politiques de session**, qui sont incluses dans le cadre d'une demande `AssumeRole`. Les politiques de session s'appliquent uniquement à la session donnée, définissant plus en détail les autorisations dont dispose l'utilisateur, en plus de celles accordées par la politique de groupe et de compartiment.



Il n'y a aucune différence de priorité entre les stratégies de groupe, de compartiment et de session.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l'intérieur de chaque règle se trouve un ensemble d'énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)

- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction
- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d'exécuter <action> sur <ressource> lorsque <condition> s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	Vous pouvez autoriser les utilisateurs, groupes et comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte peut accéder aux ressources qui lui sont propres. Le directeur : • <code>"Principal": ""</code> Correspond à tout le monde, y compris aux requêtes anonymes (non signées) • <code>"Principal": { "AWS": "*" }</code> correspond à toute identité ou utilisateur authentifié (ne correspond pas aux requêtes anonymes) • S'applique uniquement aux stratégies de compartiment • Le principal est le ou les comptes/utilisateurs auxquels les autorisations sont accordées ou refusées Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.

Élément	Description
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie doit être appliquée.

Dans l'élément action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond à des autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

Dans l'élément principal, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal": ""
```

```
"Principal": {"AWS": ""}
```

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner aux Principals, au groupe admin `federated-group/admin` et au groupe financier `federated-group/finance`, les autorisations d'effectuer l'action `s3:ListBucket` sur le compartiment nommé `mybucket` et l'action `s3:GetObject` sur tous les objets de ce compartiment.

```
{
  "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 stratégie de compartiment a une taille limite de 20,480 octets et la stratégie de groupe a une taille limite de 5,120 octets.

Cohérence au niveau des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont 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 règles. Par défaut, toutes les mises à jour des règles de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, vous pouvez souhaiter qu'une modification de règle de compartiment soit disponible en cas de panne sur le site.

Dans ce cas, vous pouvez définir l'`Consistency-Control` en-tête dans la demande PutBucketPolicy ou utiliser la demande de cohérence PUT Bucket. Lorsqu'une règle de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires en raison de la mise en cache des règles.



Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de rétablir la valeur d'origine du paramètre de niveau du compartiment lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de compartiment utiliseront le paramètre modifié.

Quelle est la politique de session ?

Une politique de session est une politique d'accès qui restreint temporairement les autorisations disponibles pendant une session spécifique, par exemple lorsqu'un utilisateur assume un groupe. Une politique de session

ne peut autoriser qu'un sous-ensemble d'autorisations et ne peut pas accorder d'autorisations supplémentaires. Le groupe lui-même pourrait avoir des autorisations plus larges.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour correspondre à zéro ou plus de caractères dans la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé de l'objet, doivent être encodés en JSON UTF-8 ou à l'aide des séquences d'échappement JSON \u. L'encodage en pourcentage n'est pas pris en charge.

"Syntaxe RFC 2141 URN"

Le corps de requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

- Chaque instruction de stratégie nécessite un élément ressource. Dans une stratégie, les ressources sont signalées par l'élément `Resource`, ou, alternativement, `NotResource` pour exclusion.
- Vous spécifiez des ressources avec une ressource S3 ARN. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de règles à l'intérieur de la clé d'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de la ressource peut spécifier un compartiment qui n'existe pas encore lors de la création d'une stratégie de groupe.

Spécifiez les entités de gestion dans une stratégie

Utilisez l'élément principal pour identifier l'utilisateur, le groupe ou le compte locataire qui est autorisé/refusé l'accès à la ressource par l'instruction de stratégie.

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique dans une stratégie de groupe n'ont pas besoin de l'élément principal car le groupe est considéré comme le principal.
- Dans une police, les principaux sont désignés par l'élément « principal » ou par l'élément « noPrincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root et tous les utilisateurs du compte :

```
"Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« gestionnaires ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": "*"
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-  
eb6b9e546013
```

Par exemple, supposons qu'Alex quitte l'organisation et que le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et se voit attribuer le même `Alex` nom d'utilisateur, le nouvel utilisateur peut involontairement hériter des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, l'élément action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.



Amazon S3 utilise désormais l'autorisation `s3:PutReplicationConfiguration` pour les actions `PutBucketReplication` et `DeleteBucketReplication`. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.



Une suppression est effectuée lorsqu'une entrée est utilisée pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	CreateBucket	Oui. Remarque : utiliser uniquement dans la stratégie de groupe.
s3>DeleteBucket	DeleteBucket	
s3>DeleteBucketMetadataNotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBuckeReplication	Oui, des autorisations séparées pour PUT et DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui
s3:GetBucketLocation	GetBuckeLocation	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui
s3:GetBuckenotification	GetBucketNotifationConfiguration	
s3:GetBuckeObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecyclConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationTM	GetBuckeReplication	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:ListAllMyseaux	- Listseaux - DÉCOUVREZ l'utilisation du stockage	Oui, pour OBTENIR l'utilisation du stockage. Remarque : utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	- GetObject - Godet principal - Objet principal - ListObjects	
s3:ListBuckMultipartUploads	ListMultipartUploads	
s3:ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui
s3:PutBuckeCORS	- DeleteBuckeCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBuckeEncryption - PutBucketEncryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui
s3:PutBuckenotification	PutBucketNotifationConfiguration	
s3:PutBuckObjectLockConfiguration	- CreateBucket avec l' `x-amz-bucket-object-lock-enabled: true` en-tête de requête (nécessite également l'autorisation s3:CreateBucket) - PutObjectLockConfiguration	
s3:PutBuckePolicy	PutBuckePolicy	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBucketTagging	- DeleteBucketTagging† - Étiquetage PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - PutBucketLifecycleConfiguration	
s3:PutReplicationTM	PutBucketReplication	Oui, des autorisations séparées pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	AbortMultipartUpload	
s3:BypassGovernanceRetention	- DeleteObject - DeleteObjects - PutObjectRetention	
s3>DeleteObject	- DeleteObject - DeleteObjects	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (une version spécifique de l'objet)	
s3>DeleteObjectVersion	DeleteObject (une version spécifique de l'objet)	
s3:GetObject	- GetObject - Objet principal - SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (une version spécifique de l'objet)	
s3:GetObjectVersion	GetObject (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	ListParts	
s3:PutObject	• Objet de copie • CompleteMultipartUpload • CreateMultipartUpload • PutObject • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	Marquage PutObject	
s3:PutObjectVersionTagging	PutObjectTagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	• CompleteMultipartUpload • Objet de copie • DeleteObjectTagging • PutObject • Marquage PutObject	Oui
s3:RestoreObject	Objet de restauration	

Utilisez l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
 - Si un objet existant se trouve sur le même chemin :
 - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
 - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
 - Si la gestion des versions S3 est activée, le paramètre deny empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet d'un objet et ses versions non actuelles.
 - Si aucun objet existant n'est trouvé, cette autorisation est sans effet.
- Lorsque cette autorisation est absente, l'effet est le même que si Allow était activé.



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.

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

Les conditions utilisent des paires de clé-valeur pour l'évaluation. Un élément condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc condition utilise le format suivant :

```
Condition: {  
  condition_type: {  
    condition_key: condition_values
```

Dans l'exemple suivant, la condition ipaddress utilise la clé condition SourceIp.

```
"Condition": {  
  "IpAddress": {  
    "aws:SourceIp": "54.240.143.0/24"  
    ...  
  },  
  ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance niée (ignore le cas).
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure des caractères génériques * et ?.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure des caractères génériques * et ?.
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une touche à une valeur numérique basée sur une correspondance « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur une correspondance « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur une correspondance « inférieure à ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur une correspondance « inférieure ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur une correspondance « vrai ou faux ».

Opérateurs de condition	Description
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.
SiExiste	Ajouté à tout opérateur de condition, à l'exception de la condition Null, pour vérifier l'absence de cette clé de condition. Renvoie TRUE si la clé de condition n'est pas présente.

Touches de condition prises en charge

Touches condition	Actions	Description
aws:Sourcelp	Opérateurs IP	Comparée à l'adresse IP à partir de laquelle la requête a été envoyée. Peut être utilisée pour les opérations sur les compartiments ou les objets. Remarque : Si la requête S3 a été envoyée via le service Load Balancer sur les nœuds d'administration et les nœuds de passerelle, cela correspond à l'adresse IP en amont du service Load Balancer. Remarque : Si un équilibreur de charge tiers non transparent est utilisé, la comparaison porte sur l'adresse IP de cet équilibreur. Tout X-Forwarded-For en-tête est ignoré car sa validité ne peut être vérifiée.
aws:nom d'utilisateur	Ressource/identité	Comparé au nom d'utilisateur de l'expéditeur à partir duquel la requête a été envoyée. Peut être utilisé pour les opérations sur les compartiments ou les objets.
s3:délimiteur	s3:ListBucket et s3:permissions ListBuckeVersions	Compare au paramètre délimiteur spécifié dans une requête ListObjects ou ListObjectVersions.

Touches condition	Actions	Description
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Nécessite que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:touches max	s3:ListBucket et s3:permissions ListBuckeVersions	Se compare au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : mode de verrouillage d'objet	s3:PutObject	Comparable à la <code>object-lock-mode</code> développé à partir de l'en-tête de requête dans les requêtes PutObject, CopyObject et CreateMultipartUpload.
s3 : mode de verrouillage d'objet	s3:PutObjectRetention	Comparable à la <code>object-lock-mode</code> développé à partir du corps XML dans la demande PutObjectRetention.
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObject	Compare à la date de conservation jusqu'à spécifiée dans l'en-tête de la demande ou calculée à <code>x-amz-object-lock-retain-until-date</code> partir de la période de conservation par défaut du compartiment pour s'assurer que ces valeurs sont dans la plage autorisée pour les demandes suivantes : • PutObject • Objet de copie • CreateMultipartUpload

Touches condition	Actions	Description
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObjectRetention	Compare à la date de conservation jusqu'à spécifiée dans la demande PutObjectRetention pour s'assurer qu'elle se trouve dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:permissions ListBuckeVersions	Se compare au paramètre de préfixe spécifié dans une requête ListObjects ou ListObjectVersions, ou à la clé spécifiée pour GetObject ou HeadObject.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Nécessite une clé et une valeur de balise spécifiques lorsque la requête d'objet inclut un étiquetage.
s3:x-amz-copy-source	s3:PutObject	Comparé à l'en-tête x-amz-copy-source développé à partir de l'en-tête de requête dans la requête PutObject et UploadPartCopy.
s3:x-amz-algorithme-client-de-chiffrement-côté-serveur-	s3:PutObject	Comparable à la sse-customer-algorithm ou à la copy-source-sse-customer-algorithm développé à partir de l'en-tête de requête dans les requêtes PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy et CompleteMultipartUpload.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règles dans l'`Resource`élément et dans des comparaisons de chaînes dans l'`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 condition :

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```


Variable	Description
<code>\${aws:SourceIp}</code>	Utilise la touche SourceIp comme variable fournie.
<code>\${aws:username}</code>	Utilise la clé de nom d'utilisateur comme variable fournie.
<code>\${s3:prefix}</code>	Utilise la clé de préfixe spécifique au service comme variable fournie.
<code>\${s3:max-keys}</code>	Utilise la touche max-keys spécifique au service comme variable fournie.
<code>\${*}</code>	Caractère spécial. Utilise le caractère comme caractère littéral *.
<code>\${?}</code>	Caractère spécial. Utilise le caractère comme un caractère littéral ?.
<code>\${\$}</code>	Caractère spécial. Utilise le caractère comme caractère littéral \$.

Créez des règles nécessitant une gestion spéciale

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou dangereuses pour les opérations continues, telles que le verrouillage de l'utilisateur racine du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des règles qu'Amazon, mais tout aussi stricte lors de l'évaluation des règles.

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La stratégie accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations de placer des objets.	Godet	Valide. Les objets appartiennent au compte créateur et la stratégie du compartiment ne s'applique pas. Le compte créateur doit accorder les autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès (ACL) d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

Vous pouvez créer des compartiments WORM (Write-once, Read-many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objets S3. Vous configurez les compartiments WORM pour permettre la création de nouveaux objets et empêcher les écrasements ou la suppression de contenu existant. Utilisez l'une des approches décrites ici.

Pour vous assurer que les écrasements sont toujours refusés, vous pouvez :

- 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 suivantes et les règles S3 :
 - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
 - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
 - Ajoutez une opération PutObject ALLOW à la règle S3.



Le fait de définir DeleteObject sur REFUSER 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 contre)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B: Remplacements séquentiels terminés (protégés contre)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informations associées

- ["Gestion des objets par les règles StorageGRID ILM"](#)
- ["Exemples de politiques de compartiments"](#)
- ["Exemples de stratégies de groupe"](#)
- ["Exemple de politique de session"](#)
- ["Gestion des objets avec ILM"](#)
- ["Utilisez un compte de locataire"](#)

Exemple de stratégie de session de l'API REST StorageGRID S3

Utilisez l'exemple suivant pour créer une stratégie de session StorageGRID .

Exemple : configurer une politique de session qui autorise la récupération d'objets

Dans cet exemple, le principal de la session est uniquement autorisé à récupérer des objets du bucket1. Toutes les autres actions sont implicitement refusées, sauf pour les actions spécifiques à StorageGRID, telles que l'utilisation de la permission ["s3:PutOverwriteObject"](#). La politique de session peut être fournie sous forme de fichier JSON lors de l'appel à l'API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Exemples de stratégie de compartiment de l'API REST StorageGRID S3

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments.

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Pour configurer une stratégie de compartiment, utilisez l'API PutBucketPolicy S3 au moyen de l'un des outils suivants :

- ["Gestionnaire de locataires"](#).
- CLI AWS utilisant cette commande (voir ["Opérations sur les compartiments"](#)) :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Dans StorageGRID, le principal :

- `"Principal": "*"``` Correspond à tout le monde, y compris aux requêtes anonymes (non signées)
- `"Principal": { "AWS": "*" }` correspond à toute identité ou utilisateur authentifié (ne correspond pas aux requêtes anonymes)
- S'applique uniquement aux stratégies de compartiment
- Le principal est le ou les comptes/utilisateurs auxquels les autorisations sont accordées ou refusées

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier les objets dans le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique peut ne pas être particulièrement utile, car personne, à l'exception de la racine du compte, ne peut écrire dans le compartiment.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}

```

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié est autorisé à accéder à un compartiment, tandis que tous les utilisateurs d'un autre compte spécifié sont uniquement autorisés à répertorier le compartiment et à effectuer des opérations `GetObject` sur les objets du compartiment en commençant par le `shared/` préfixe de clé d'objet.



Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment s'applique à ces objets.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment, alors que seuls les utilisateurs appartenant au groupe Marketing du compte spécifié ont un accès complet.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : autoriser tout le monde à lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

Exemple : autoriser un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder entièrement au `examplebucket` compartiment et à ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, l'`Deny` effet de PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage d'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 stratégie de groupe pour l'API REST S3 de StorageGRID

Utilisez les exemples de cette section pour créer des stratégies d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas d'`Principal` élément dans la règle car elle est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

Lorsque vous ajoutez ou modifiez un groupe dans le Gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont les membres de ce groupe auront accès. Voir "[Créez des groupes pour un locataire S3](#)".

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.

Les utilisateurs du Gestionnaire de locataires disposant de l'autorisation gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.

- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Exemple : autorisez les membres du groupe à accéder entièrement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

Opérations S3 suivies dans les journaux d’audit de StorageGRID

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 informations détaillées sur les opérations relatives aux compartiments et aux objets.

Les opérations des compartiments sont suivies dans les journaux d’audit

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketTagging
- DeleteObjects
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketTagging
- Godet principal
- ListObjects
- ListObjectVersions

- METTEZ le godet en conformité
- PutBucketLifecycleConfiguration
- PutBucketPolicy
- Étiquetage PutBucketTagging
- PutBucketVersioning

Opérations d'objet suivies dans les journaux d'audit

- CompleteMultipartUpload
- Objet de copie
- DeleteObject
- GetObject
- Objet principal
- PutObject
- Objet de restauration
- SelectObject
- UploadPart (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)

Informations associées

- ["Accéder au fichier journal d'audit"](#)
- ["Écrire des messages d'audit client"](#)
- ["Messages d'audit de lecture du client"](#)

Utilisation de l'API REST Swift (fin de vie)

Prise en charge de l'API REST Swift dans StorageGRID

La prise en charge de l'API Swift est arrivée en fin de vie et sera supprimée dans une prochaine version.



Les détails SWIFT ont été supprimés de cette version du site doc. Voir ["StorageGRID 11.8 : utilisez l'API REST Swift"](#).

Surveillance et dépannage d'un système StorageGRID

Surveiller le système StorageGRID

Utiliser AutoSupport

Découvrez AutoSupport dans StorageGRID

La fonctionnalité AutoSupport permet à StorageGRID d'envoyer des packages d'état et d'intégrité au support technique NetApp.

L'utilisation AutoSupport permet de résoudre les problèmes plus rapidement. Le support technique peut surveiller les besoins de stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. En option, AutoSupport peut envoyer des colis vers une destination supplémentaire.

StorageGRID propose deux types de AutoSupport :

- **StorageGRID AutoSupport** signale des problèmes de logiciel StorageGRID. Activé par défaut lors de la première installation de StorageGRID. Vous pouvez le ["Modifier la configuration AutoSupport par défaut"](#) faire 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.

- **Le matériel de l'appareil AutoSupport** signale les problèmes de l'appareil StorageGRID. Vous devez ["Configurer le matériel AutoSupport sur chaque appliance"](#).

Qu'est-ce que Digital Advisor ?

Active IQ Digital Advisor (également appelé Digital Advisor) est une solution cloud qui exploite l'analyse prédictive et l'expertise issue de la base installée de NetApp. Ses évaluations continues des risques, ses alertes prédictives, ses recommandations prescriptives et ses actions automatisées vous aident à prévenir les problèmes avant qu'ils ne surviennent, ce qui améliore la santé et la disponibilité du système.

Vous devez activer AutoSupport si vous souhaitez utiliser les tableaux de bord et la fonctionnalité Digital Advisor sur le site de support NetApp.

["Documentation Digital Advisor"](#)

Informations incluses dans le package AutoSupport

Un package AutoSupport contient les fichiers et détails suivants.

Nom du fichier	Champs	Description
AUTOSUPPORT-HISTORY.XML	Numéro de séquence AutoSupport + destination pour ce AutoSupport + État de livraison + tentatives de livraison + objet AutoSupport + URI de livraison + dernière erreur + Nom de fichier AutoSupport PUT + heure de génération + taille compressée AutoSupport + taille décompressée AutoSupport + durée totale de collecte (ms)	Fichier d'historique AutoSupport.
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + adresse de support + Etat 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 le AutoSupport à la demande si activé ou désactivé.
BUCKETS.XML	ID de compartiment + ID de compte + version de build + Configuration de contrainte d'emplacement + conformité activée + Configuration de conformité + verrouillage d'objet S3 activé + Configuration de verrouillage d'objet S3 + Configuration de cohérence + CORS activée + Configuration de l'identification de compartiment activée + heure du dernier accès activée + Configuration de la stratégie + Notifications activées + Configuration de miroir cloud activée + Configuration de la recherche activée + Configuration de l'étiquetage de compartiment activée + Configuration de l'étiquetage de compartiment activée	Fournit des informations de configuration et des statistiques au niveau du compartiment. Les services de plateforme, la conformité et la cohérence des compartiments sont des exemples de configuration de compartiment.

Nom du fichier	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 grid, l'espace réservé aux métadonnées, les paramètres de configuration de l'ensemble de la grille (conformité, verrouillage objet S3, compression d'objet, alertes, syslog et configuration ILM), les détails du profil de code d'effacement, le nom DNS et " Nom du NMS ".
GRID-SPEC.XML	Spécifications de grille, XML brut	Permet de configurer et de déployer StorageGRID. Contient les spécifications du grid, l'adresse IP du serveur NTP, l'adresse IP du serveur DNS, la topologie 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 grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, terminées, ayant échoué et en attente de la grille.
GRID.JSON	Grid + révision + version du logiciel + Description + Licence + mots de passe + DNS + NTP + sites + nœuds	Informations de grille.
ILM-CONFIGURATION.XML	ID d'attribut + Nom d'attribut + valeur + Index + ID de table + Nom de table	Liste des attributs des configurations ILM.
ILM-STATUS.XML	Nœud + chemin de service + ID d'attribut + Nom d'attribut + valeur + Index + ID de table + Nom de table	Fichier d'informations de metrics ILM. Les taux d'évaluation ILM pour chaque nœud et les metrics de la grille sont indiqués.
ILM.XML	XML brut ILM	Fichier de règles actif ILM. Contient des informations détaillées sur les règles ILM actives, telles que l'ID de 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 du fichier	Champs	Description
MANIFEST.XML	Ordre de collecte + nom de 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 des métadonnées AutoSupport et une brève description de tous les fichiers AutoSupport.
NMS-ENTITÉS.XML	Index des attributs + OID de l'entité + ID du nœud + ID du modèle du périphérique + version du modèle du périphérique + Nom de l'entité	Groupe et entités de service dans " Arborescence NMS ". Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.
OBJECTS-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 d'analyse en arrière-plan, le transfert actif, le taux de transfert, le total des transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la tentative de réparation, la vitesse 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 les détails suivants pour chaque nœud : type de plateforme, système d'exploitation, mémoire installée, mémoire disponible, connectivité du stockage, numéro de série du châssis de l'appliance de stockage, nombre de disques défaillants 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 mesures Reaper de la base de données, la durée de réparation des segments, la durée des travaux de réparation, les redémarrages automatiques des travaux et la fin automatique des travaux.

Nom du fichier	Champs	Description
STORAGE-GRADES.XML	ID du niveau de stockage + Nom du niveau de stockage + ID du nœud de stockage + chemin du nœud de stockage	Fichier de définitions des niveaux de stockage pour chaque nœud de stockage.
SUMMARY-ATTRIBUTES.XML	OID groupe + chemin groupe + ID attribut résumé + Nom attribut résumé + valeur + Index + ID table + Nom table	Données générales sur l'état du système qui récapitule les informations d'utilisation de StorageGRID. Fournit des informations telles que le nom de la grille, le nom des sites, le nombre de nœuds de stockage par grid et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions du support logiciel et des détails des opérations S3.
SYSTEM-ALERTS.XML	Nom + gravité + Nom du nœud + Statut de l'alerte + Nom du site + heure de déclenchement de l'alerte + heure de résolution de l'alerte + ID de la 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 POST (ms) + OPTIONS temps moyen (ms)	Statistiques basées sur les agents utilisateur 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.
DONNÉES-EN-TÊTE-X.	X-NetApp-asup-generated-on + X-NetApp-asup-hostname + X-NetApp-asup-os-version + X-NetApp-asup-num-série + X-NetApp-asup-subject + X-NetApp-asup-ID-système + X-NetApp-asup-nom-modèle +	Données d'en-tête AutoSupport.

Configurer AutoSupport dans StorageGRID

La fonctionnalité AutoSupport permet à votre système StorageGRID d'envoyer des messages périodiques et déclenchés par des événements concernant l'état et la santé au support technique afin de permettre une surveillance proactive et un dépannage. StorageGRID AutoSupport permet également l'utilisation de Digital Advisor pour des recommandations prédictives.

Par défaut, les fonctionnalités hebdomadaires et déclenchées par événement AutoSupport sont activées pour les systèmes StorageGRID logiciels lors de la première installation de StorageGRID. Cependant, vous devez [Configurer le matériel AutoSupport](#) sur chaque appliance. Au besoin, 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.

Avant de commencer

- Vous êtes connecté au Grid Manager sur le nœud d'administration principal à l'aide d'["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).
- Si vous utilisez HTTPS pour envoyer des packages AutoSupport, vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit ["utilisation d'un serveur proxy"](#) (les connexions entrantes ne sont pas requises).
- Si HTTP est sélectionné sur la page AutoSupport de StorageGRID, vous devez ["configurez un serveur proxy"](#) 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 paquets AutoSupport, vous avez ["configuré un serveur de messagerie"](#).

Description de la tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire**: Envoyer automatiquement des paquets AutoSupport une fois par semaine. Paramètre par défaut : activé.
- **Déclenché par un événement** : envoie automatiquement des paquets AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : activé.
- **À la demande** : permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des paquets AutoSupport, ce qui est utile lorsqu'ils travaillent activement à un problème (nécessite le protocole de transmission AutoSupport HTTPS). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des paquets AutoSupport à tout moment.
- **Collecte de journaux**:["collecter manuellement les fichiers journaux et les données système et envoyer un package AutoSupport"](#) .

Configurer AutoSupport

Pour modifier la configuration d'installation par défaut de AutoSupport, ou pour configurer le matériel AutoSupport sur chaque appliance StorageGRID :

Étapes

1. Sélectionnez **Support > Outils > * AutoSupport* > Paramètres**.
2. Sélectionnez le protocole que vous souhaitez utiliser 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 vous le souhaitez [Activez la fonction AutoSupport On Demand](#), vous devez utiliser HTTPS.
 - **HTTP** : si vous sélectionnez HTTP, vous devez "[configurer un serveur proxy](#)" pour transférer les 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 paquets AutoSupport soient envoyés par e-mail. Vous devez d'abord "[configurer un serveur de messagerie](#)".

Le protocole que vous avez défini est utilisé pour l'envoi de tous les paquets AutoSupport sauf AutoSupport on Demand, qui nécessite le protocole HTTPS.
3. Si vous avez sélectionné **HTTPS**, choisissez d'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 paquets AutoSupport est sécurisée. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
 - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple lorsqu'il y a un problème temporaire avec un certificat.
4. Si vous avez sélectionné **SMTP**, utilisez le champ **Expéditeur** pour saisir l'adresse du serveur de messagerie que vous avez configuré précédemment.
5. Sélectionnez **Enregistrer**. Tous les paquets hebdomadaires, déclenchés par l'utilisateur et déclenchés par des événements sont envoyés à l'aide du protocole sélectionné.

Désactivez 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 paquet AutoSupport hebdomadaire sera envoyé, allez à l'onglet **AutoSupport > Résultats**. Dans la section **AutoSupport hebdomadaire**, examinez la valeur de **prochaine heure planifiée**.

Vous pouvez désactiver à tout moment l'envoi automatique de packages AutoSupport hebdomadaires.

Étapes

1. Sélectionnez **Support > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactivez la fonction AutoSupport déclenchée par un événement

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique toutes les heures.

Vous pouvez désactiver les AutoSupport déclenchées par un événement à tout moment.

Étapes

1. Sélectionnez **Support > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Activer AutoSupport** déclenché par un événement.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport on Demand

AutoSupport On Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

AutoSupport On Demand est désactivé par défaut. L'activation de cette fonction permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport. Le support technique peut également définir l'intervalle d'interrogation pour les requêtes AutoSupport On Demand.

Le support technique ne peut ni activer ni désactiver AutoSupport On Demand.

Étapes

1. Sélectionnez **Support > Outils > * AutoSupport* > Paramètres**.
2. Sélectionnez le **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport On Demand**.
5. Sélectionnez **Enregistrer**.

AutoSupport On Demand est activé et le support technique peut envoyer des demandes AutoSupport On Demand à StorageGRID.

Désactive les vérifications des mises à jour logicielles

Par défaut, StorageGRID contacte NetApp pour déterminer si des mises à jour logicielles sont disponibles pour votre système. Si un correctif StorageGRID ou une nouvelle version est disponible, la nouvelle version s'affiche sur la page mise à niveau StorageGRID.

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'un accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **Support > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Rechercher les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les packages d'état et de santé 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 des paquets AutoSupport, consultez les instructions pour [configurer 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. Spécifiez les éléments suivants :

Nom d'hôte

Nom d'hôte ou adresse IP du serveur d'un serveur de destination AutoSupport supplémentaire.



Vous ne pouvez entrer qu'une destination supplémentaire.

Port

Port utilisé pour se connecter à un serveur de destination AutoSupport supplémentaire. La valeur par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS.

Validation du certificat

Indique 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 si 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 de l'autorité de certification.
 - b. Téléchargez le fichier de certificat de l'autorité de certification.

Les métadonnées du certificat de l'autorité de certification s'affichent.

5. Sélectionnez **Enregistrer**.

Tous les packages AutoSupport hebdomadaires, déclenchés par des événements et déclenchés par l'utilisateur seront envoyés vers la destination supplémentaire.

configurez AutoSupport pour les appliances

AutoSupport for Appliances signale les problèmes liés au matériel StorageGRID. StorageGRID AutoSupport signale les problèmes liés au logiciel StorageGRID, à l'exception du SGF6112, StorageGRID AutoSupport signale les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appliance, à l'exception du SGF6112, qui ne nécessite pas de configuration supplémentaire. AutoSupport est implémenté différemment pour les appliances de services et de stockage.

SANtricity vous permet d'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 appliances SG6000 et SG5700 ["Configurez AutoSupport dans SANtricity System Manager"](#)

AutoSupport packages des appliances de la série E peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans ["SANtricity System Manager"](#).

StorageGRID AutoSupport ne signale pas de problèmes matériels, tels que des pannes de module DIMM ou de carte d'interface hôte (HIC). Cependant, certaines défaillances de composant peuvent ["alertes matérielles"](#) se déclencher. Pour les appliances StorageGRID dotées d'un contrôleur BMC (Baseboard Management Controller), vous pouvez configurer des interruptions SNMP et des e-mails pour signaler les défaillances matérielles :

- ["Configurez les notifications par e-mail pour les alertes BMC"](#)
- ["Configurer les paramètres SNMP pour le contrôleur BMC"](#)

Informations associées

- ["Ports utilisés pour les communications externes"](#)
- ["Support NetApp"](#)

Déclencher manuellement un AutoSupport package dans StorageGRID

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un pack AutoSupport.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous disposez 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 déclenché 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.

3. Après 1 minute, actualisez la page AutoSupport dans votre navigateur pour accéder aux résultats les plus récents.



De plus, vous pouvez ["collecter des fichiers journaux et des données système plus complets"](#) et envoyez-les au site de support NetApp.

Comment StorageGRID gère les échecs de paquets AutoSupport

Consultez la liste des actions que StorageGRID effectue si une tentative d'envoi d'un package AutoSupport échoue.

StorageGRID effectue différentes actions selon le type de AutoSupport package. Vous pouvez consulter l'état des packages AutoSupport en sélectionnant **Support > Outils > AutoSupport > Résultats**.

Lorsque le paquet AutoSupport ne parvient pas à envoyer, "failed" apparaît sur l'onglet **Results** de la page **AutoSupport**.



Si vous avez configuré un serveur proxy pour transférer les paquets AutoSupport à NetApp, ["vérifiez que les paramètres de configuration du serveur proxy sont corrects"](#).

Défaillance hebdomadaire du package AutoSupport

Si l'envoi d'un pack AutoSupport hebdomadaire échoue, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut de résultat le plus récent pour réessayer.
2. Tente de renvoyer le package AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échec d'envoi, met à jour l'attribut de résultat le plus récent sur échec.
4. Tente d'envoyer à nouveau un pack AutoSupport à la prochaine heure programmée.
5. Maintient le programme AutoSupport normal si le package échoue parce que le service NMS est indisponible et si un package est envoyé avant sept jours.
6. Lorsque le service NMS est de nouveau disponible, envoie un package AutoSupport immédiatement si un package n'a pas été envoyé pendant sept jours ou plus.

Défaillance du package AutoSupport déclenché par l'utilisateur ou l'événement

Si un package AutoSupport déclenché par l'utilisateur ou un événement ne parvient pas à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir de 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. Ne tente pas d'envoyer à nouveau le pack.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si le protocole SMTP est sélectionné, 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"](#).

Corrigez une défaillance du package AutoSupport

En cas d'échec et si le protocole SMTP est 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 s'afficher sur la page AutoSupport : les paquets AutoSupport ne peuvent pas être envoyés via le protocole SMTP en raison de paramètres incorrects sur la page Serveur de messagerie.

Envoyez des packages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer des packages AutoSupport du Gestionnaire système SANtricity E-Series au support technique via un nœud d'administration StorageGRID plutôt que le port de gestion de l'appliance de stockage.

Pour plus d'informations sur l'utilisation de AutoSupport avec les appliances E-Series, reportez-vous à la section ["Matériel E-Series AutoSupport"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Administrateur de l'appliance de stockage ou autorisation d'accès racine"](#).
- Vous avez configuré SANtricity AutoSupport :
 - Pour les appliances SG6000 et SG5700 ["Configurez AutoSupport dans SANtricity System Manager"](#)



Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

Description de la tâche

Les packages AutoSupport E-Series contiennent des informations détaillées 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 le Gestionnaire système SANtricity pour transmettre des packages AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les paquets AutoSupport transmis de cette façon sont envoyés par le ["Nœud d'administration de l'expéditeur préféré"](#), et ils utilisent tous ceux ["paramètres du proxy d'administration"](#) qui ont été configurés dans le Gestionnaire de grille.

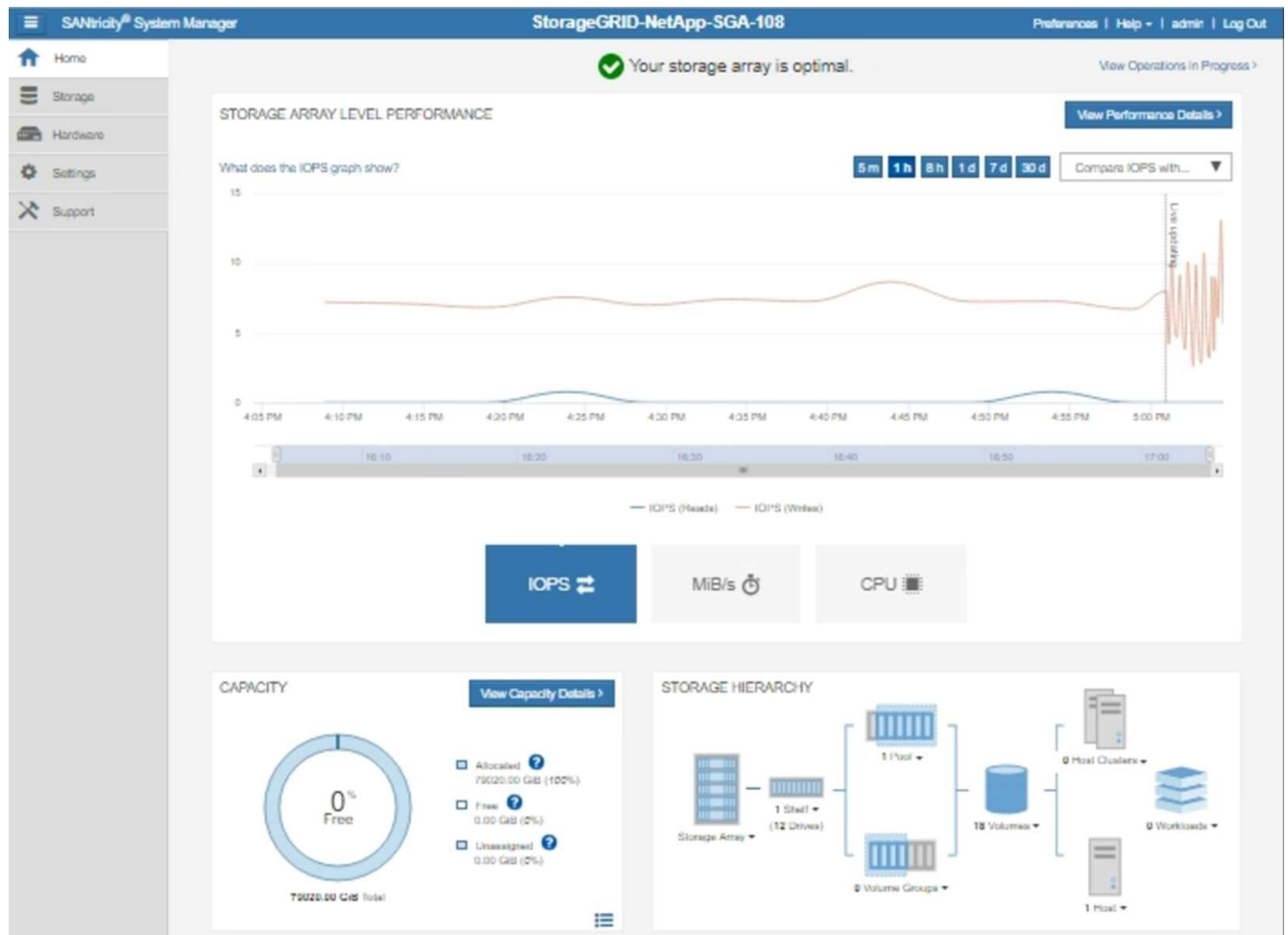


Cette procédure concerne uniquement la configuration d'un serveur proxy StorageGRID pour les packages E-Series AutoSupport. Pour plus de détails sur la configuration E-Series AutoSupport, consultez le ["Documentation NetApp E-Series et SANtricity"](#).

Étapes

1. Dans le gestionnaire de grille, sélectionnez **Nœuds**.
2. Dans la liste des nœuds de gauche, sélectionnez le nœud d'appliance de stockage à configurer.
3. Sélectionnez **SANtricity System Manager**.

La page d'accueil de SANtricity System Manager s'affiche.



4. Sélectionnez **Support** > **Centre d'assistance** > * AutoSupport*.

La page 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.

Configure AutoSupport Delivery Method

Select AutoSupport dispatch delivery method...

☒ HTTPS
☐ HTTP
☐ Email

HTTPS delivery settings [Show destination address](#)

Connect to support team...

☐ Directly ?
☒ via Proxy server ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication
☐ via Proxy auto-configuration script (PAC) ?

6. Sélectionnez **HTTPS** pour la méthode de livraison.



Le certificat qui active HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.

8. Entrez `tunnel-host` l'adresse **hôte**.

`tunnel-host` Est l'adresse spéciale permettant d'utiliser un nœud d'administration pour envoyer les packages AutoSupport E-Series.

9. Entrez `10225` 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 le cas, un message s'affiche dans une bannière verte : « votre configuration AutoSupport a été vérifiée ».

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez vos paramètres DNS et la mise en réseau StorageGRID, assurez-vous que le système "[Nœud d'administration de l'expéditeur préféré](#)" peut se connecter au site de support NetApp, puis réessayez le test.

11. Sélectionnez **Enregistrer**.

La configuration est enregistrée et un message de confirmation s'affiche : « la méthode de livraison AutoSupport a été configurée ».

Surveiller un système StorageGRID

Surveillez régulièrement votre système StorageGRID pour vous assurer qu'il fonctionne comme prévu.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[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**.

Description de la tâche

Ces instructions expliquent comment :

- "[Affichez et gérez le tableau de bord](#)"
- "[Afficher la page nœuds](#)"
- "[Surveiller régulièrement ces aspects du système :](#)"
 - "[État du système](#)"
 - "[Capacité de stockage](#)"
 - "[Gestion du cycle de vie des informations](#)"
 - "[Ressources réseau et système](#)"
 - "[Activité des locataires](#)"
 - "[Opérations d'équilibrage de la charge](#)"
 - "[Connexions de fédération de grille](#)"
- "[Gérer les alertes](#)"
- "[Afficher les fichiers journaux](#)"
- "[Configurer la gestion des journaux et le serveur syslog externe](#)"
- "[Utiliser un serveur syslog externe](#)" pour collecter des informations d'audit
- "[Utilisez SNMP pour la surveillance](#)"
- "[Modifier la priorisation des E/S](#)" pour modifier les priorités relatives des opérations d'E/S

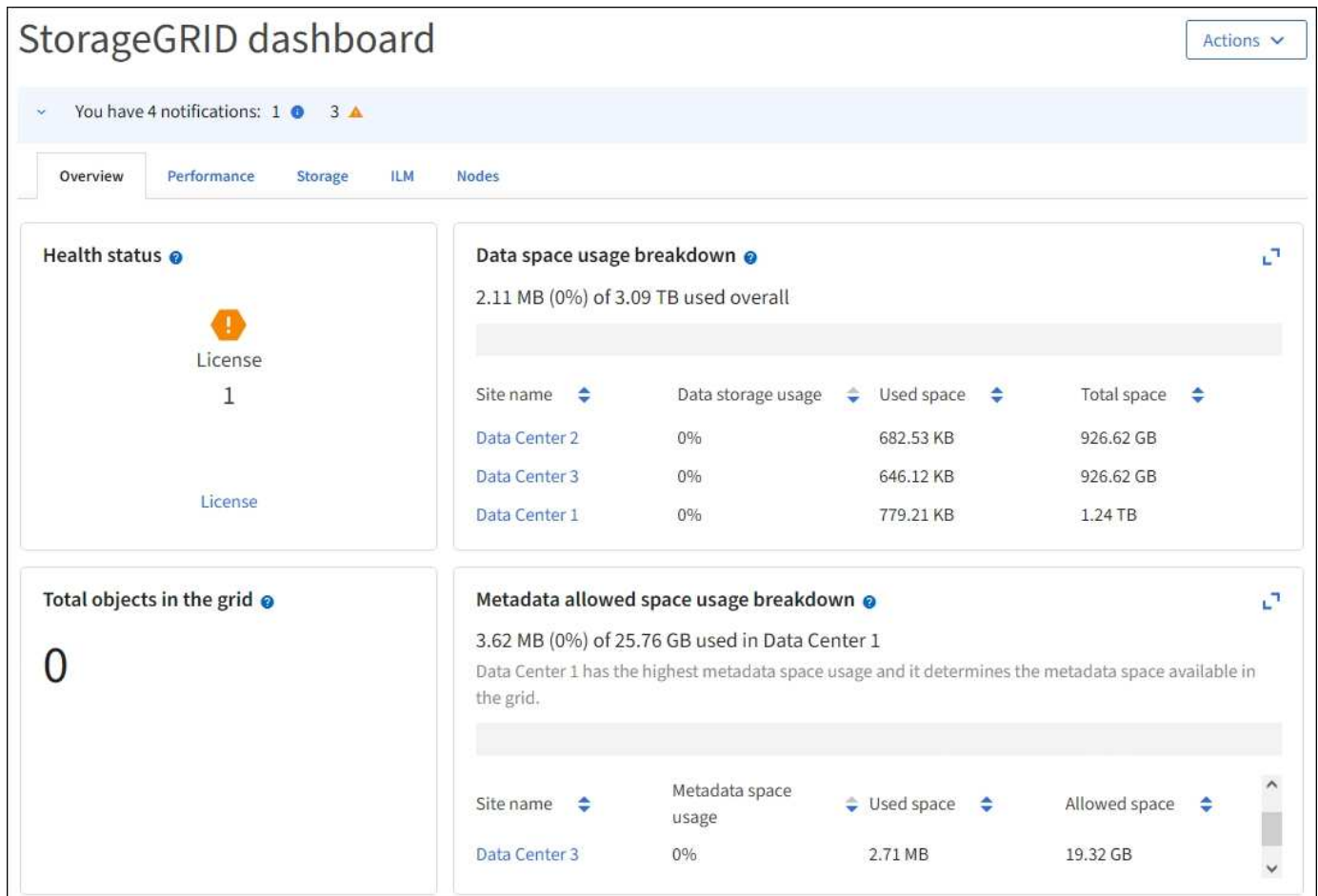
Consultez et gérez le tableau de bord dans StorageGRID

Vous pouvez utiliser le tableau de bord pour surveiller les activités du système en un coup d'œil. Vous pouvez créer des tableaux de bord personnalisés pour contrôler votre implémentation de StorageGRID.



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

Votre tableau de bord peut varier 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 qu'il est. En outre, vous pouvez créer des tableaux de bord personnalisés contenant uniquement les onglets et cartes pertinents pour la surveillance de votre implémentation de StorageGRID.

Les onglets du tableau de bord fournis par le système contiennent des cartes présentant les types d'informations suivants :

Du tableau de bord fourni par le système	Contient
Présentation	Informations générales sur la grille, telles que les alertes actives, l'utilisation de l'espace et le nombre total d'objets de la grille.
Performances	Utilisation de l'espace, stockage utilisé au fil du temps, opérations S3, durée de la demande, taux d'erreur.
Stockage	Utilisation des quotas des locataires et de l'espace logique. Prévisions de l'utilisation de l'espace pour les données utilisateur et les métadonnées.
ILM	File d'attente de gestion du cycle de vie des informations et taux d'évaluation.
Nœuds	Utilisation du CPU, des données et de la mémoire par nœud. Opérations S3 par nœud. Distribution nœud à site.

Certaines cartes peuvent être agrandies pour une meilleure lisibilité. Sélectionnez l'icône d'agrandissement  dans le coin supérieur droit de la carte. Pour fermer une carte agrandie, sélectionnez l'icône de réduction  ou sélectionnez **Fermer**.

Gestion des tableaux de bord

Si vous disposez d'un accès racine (voir "[Autorisations de groupe d'administration](#)"), vous pouvez effectuer les tâches de gestion suivantes pour les tableaux de bord :

- Créez un tableau de bord personnalisé à partir de zéro. Vous pouvez utiliser des tableaux de bord personnalisés pour contrôler quelles informations StorageGRID sont affichées et comment elles sont organisées.
- Cloner un tableau de bord pour créer des tableaux de bord personnalisés.
- Définir un tableau de bord actif pour un utilisateur. Le tableau de bord actif peut être celui fourni par le système ou un tableau de bord personnalisé.
- Définissez un tableau de bord par défaut, qui correspond à ce que tous les utilisateurs voient, à moins qu'ils n'activent leur propre tableau de bord.
- Modifiez le nom d'un tableau de bord.
- Modifiez un tableau de bord pour ajouter ou supprimer des onglets et des cartes. Vous pouvez avoir un minimum de 1 et un maximum de 20 onglets.
- Déposer un tableau de bord.



Si vous disposez d'une autre autorisation que l'accès racine, vous ne pouvez définir qu'un tableau de bord actif.

Pour gérer les tableaux de bord, sélectionnez **actions** > **gérer les tableaux de bord**.



Configurer les tableaux de bord

Pour créer un nouveau tableau de bord en clonant le tableau de bord actif, sélectionnez **actions** > **Cloner le tableau de bord actif**.

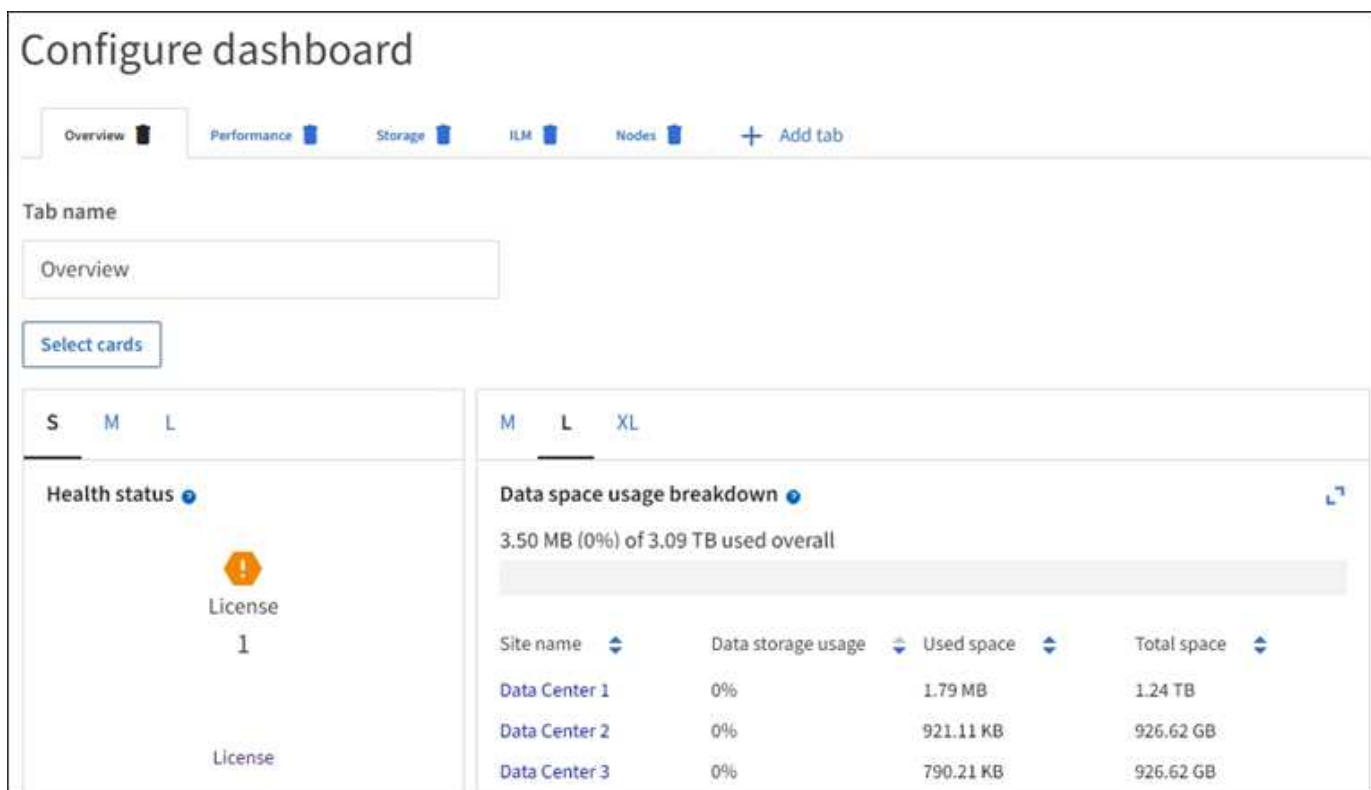
Pour modifier ou cloner un tableau de bord existant, sélectionnez **actions** > **gérer les tableaux de bord**.



Le tableau de bord fourni par le système ne peut pas être modifié ou supprimé.

Lors de la configuration d'un tableau de bord, vous pouvez :

- Ajouter ou supprimer des onglets
- Renommez les onglets et donnez des noms uniques aux nouveaux onglets
- Ajoutez, supprimez ou réorganisez (faites glisser) des cartes pour chaque onglet
- Sélectionnez la taille des cartes individuelles en sélectionnant **S**, **M**, **L** ou **XL** en haut de la carte



Afficher la page nœuds

Consultez la page des nœuds StorageGRID

Si vous avez besoin d'informations plus détaillées sur votre système StorageGRID que le

tableau de bord ne l'indique, vous pouvez utiliser la page nœuds pour afficher les mesures de la grille dans son intégralité, de chaque site de la grille et de chaque nœud d'un site.

Le tableau nœuds répertorie les informations récapitulatives pour l'ensemble de la grille, chaque site et chaque nœud. Si un nœud est déconnecté ou dispose d'une alerte active, une icône s'affiche en regard du nom du nœud. Si le nœud est connecté et ne dispose d'aucune alerte active, aucune icône n'est affichée.



Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.



Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.



Les captures d'écran illustrées 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 de la grille, l'une des icônes suivantes s'affiche en regard du nom du nœud.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue. L'alerte Impossible de communiquer avec le nœud peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. "Sélectionnez chaque alerte" et suivre les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud. Remarque : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.
	Non connecté - Arrêt administratif Pour une raison prévue, le nœud n'est pas connecté au grid. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives "Sélectionnez chaque alerte" et suivez les actions recommandées.

Si un nœud est déconnecté de la grille, une alerte sous-jacente peut apparaître, mais seule l'icône « non connecté » s'affiche. Pour afficher les alertes actives d'un nœud, sélectionnez le nœud.

Icônes d'alerte

Si une alerte est active pour un nœud, l'une des icônes suivantes s'affiche à côté du nom du nœud :

 **Critique** : Une condition anormale existe qui a interrompu le fonctionnement normal d'un nœud ou service StorageGRID. Vous devez résoudre immédiatement le problème sous-jacent. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu.

 **Majeur** : Une anomalie existe qui affecte les opérations en cours ou approche le seuil d'alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tout problème sous-jacent afin de garantir que l'anomalie ne perturbe pas le fonctionnement normal d'un nœud ou service StorageGRID.

 **Mineur** : Le système fonctionne normalement, mais une anomalie existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne se résolvent pas d'elles-mêmes afin de vous assurer qu'elles ne provoquent pas un problème plus grave.

Afficher les détails d'un système, d'un site ou d'un nœud

Pour filtrer les informations affichées dans la table nœuds, entrez une chaîne de recherche dans le champ **Search**. Vous pouvez effectuer une recherche par nom de système, nom d'affichage ou type (par exemple, entrez **gat** pour localiser rapidement tous les nœuds de passerelle).

Pour afficher les informations de la grille, du site ou du nœud :

- Sélectionnez le nom de la grille pour afficher un récapitulatif des agrégats des statistiques de l'ensemble du système StorageGRID.
- Sélectionnez un site de data Center spécifique pour afficher un résumé global des statistiques pour tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

Consultez l'onglet Vue d'ensemble StorageGRID

L'onglet Présentation fournit des informations de base sur chaque nœud. Il affiche également toutes les alertes qui affectent actuellement le nœud.

L'onglet vue d'ensemble s'affiche pour tous les nœuds.

Informations sur le nœud

La section informations sur les nœuds de l'onglet vue d'ensemble répertorie les informations de base sur le nœud.

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 de présentation 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 la "[Renommez 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 Admin, nœud Admin principal, nœud de stockage ou nœud passerelle.
- **ID** : identificateur unique du nœud, qui est également appelé UUID.
- **Etat de connexion** : l'un des trois États. L'icône de l'état le plus grave est affichée.

- **Inconnu**  : Pour une raison inconnue, le nœud n'est pas connecté à la grille, ou un ou plusieurs services sont indisponibles de façon inattendue. Par exemple, la connexion réseau entre les nœuds a été perdue, il y a une coupure de courant ou un service est indisponible. L'alerte **Unable to communicate with node** peut également être déclenchée. D'autres alertes peuvent également être actives. Cette situation requiert une attention immédiate.



Un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Dans ces cas, vous pouvez ignorer l'état Inconnu.

- **Hors service administrativement**  : Le nœud n'est pas connecté au réseau pour une raison prévue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud est en cours de redémarrage 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** : pourcentage de l'espace total utilisable pour les données d'objet qui ont été utilisées sur le nœud de stockage.
 - **Métadonnées d'objet** : pourcentage de l'espace total autorisé pour les métadonnées d'objet qui ont été utilisées sur le nœud de stockage.
- **Version du logiciel** : la version de StorageGRID installée sur le nœud.
- **Groupes HA** : pour les nœuds d'administration et de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe haute disponibilité et si cette interface est l'interface principale.
- **Adresses IP** : Les adresses IP du nœud. Sélectionnez **Afficher les adresses IP supplémentaires** pour afficher les adresses IPv4 et IPv6 du nœud ainsi que les mappages d'interface.

Alertes

La section alertes de l'onglet vue d'ensemble répertorie tous les "[alertes affectant actuellement ce nœud qui n'ont pas été neutralisées](#)". Sélectionnez le nom de l'alerte pour afficher des détails supplémentaires et les actions recommandées.

Alerts

Alert name	Severity	Time triggered	Current values
Low installed node memory	✖ Critical	11 hours ago	Total RAM size: 8.37 GB
The amount of installed memory on a node is low.			

Des alertes sont également incluses pour "états de connexion de nœud".

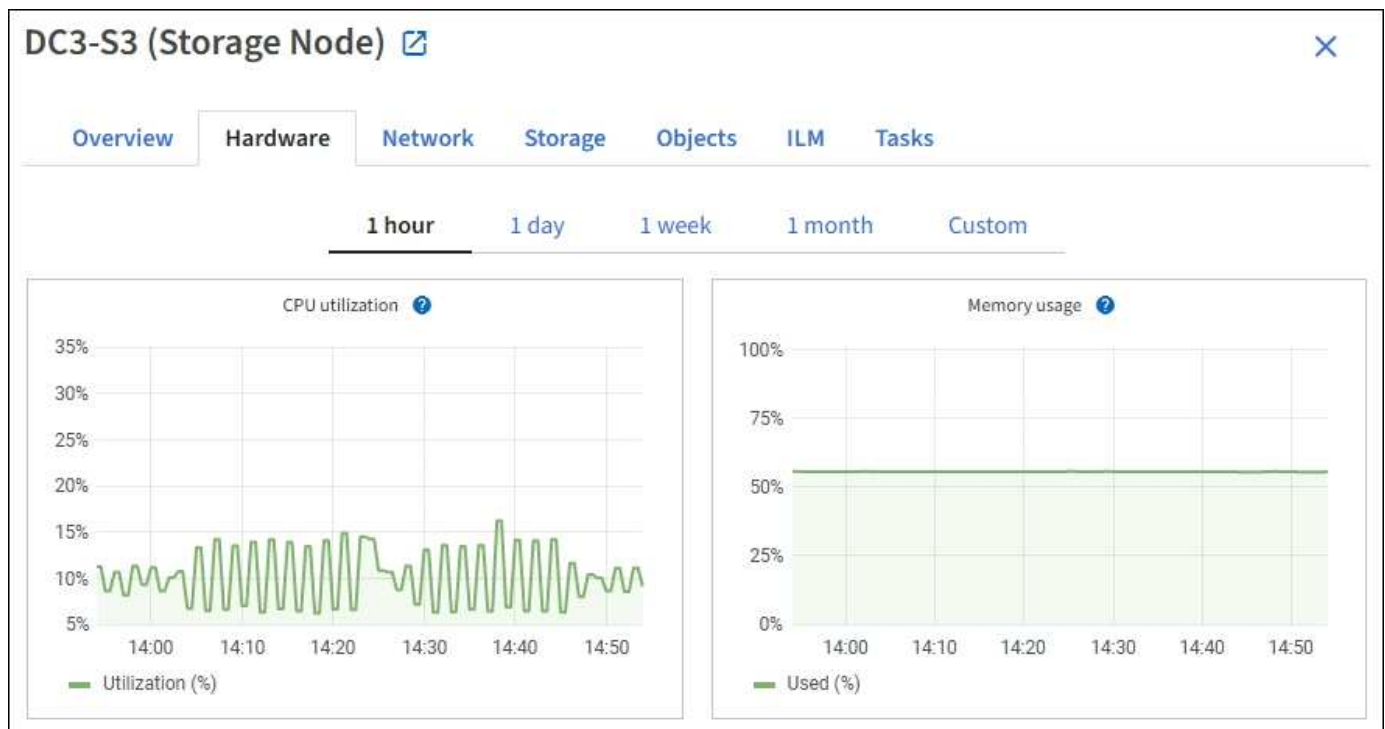
Consultez l'onglet Matériel StorageGRID

L'onglet matériel affiche l'utilisation du CPU et de la mémoire pour chaque nœud, ainsi que des informations supplémentaires sur le matériel des appliances.



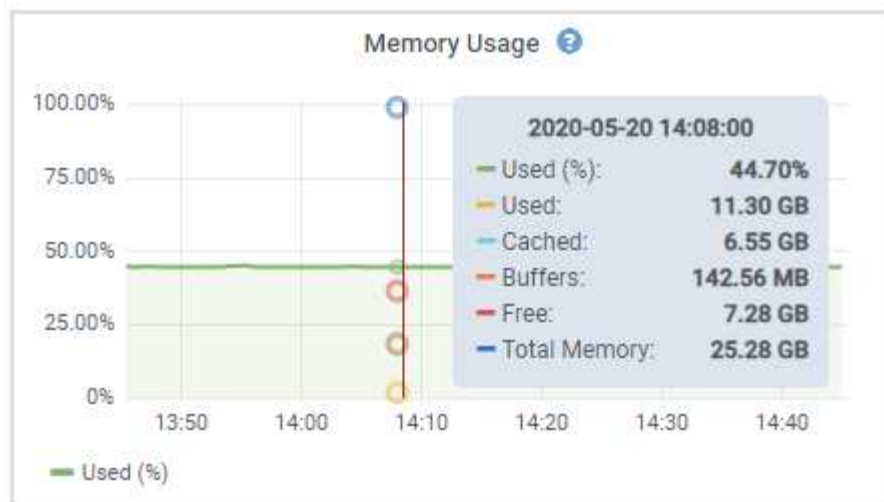
Le Gestionnaire de grille est mis à jour avec chaque version et peut ne pas correspondre aux exemples de captures d'écran de cette page.

L'onglet matériel s'affiche pour tous les nœuds.



Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour afficher des détails sur l'utilisation du CPU et de la mémoire, placez votre curseur sur chaque graphique.



Si le nœud est un nœud d'appliance, cet onglet inclut également une section contenant des informations supplémentaires sur le matériel de l'appliance.

Afficher des informations sur les nœuds de stockage de l'appliance

La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque nœud de stockage d'appliance. Vous pouvez également afficher la mémoire, le matériel de stockage, la version du firmware des contrôleurs, les ressources réseau, les interfaces réseau, les adresses réseau et de réception et de transmission des données.

Étapes

1. Sur la page nœuds, sélectionnez un nœud de stockage d'appliance.
2. Sélectionnez **vue d'ensemble**.

La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :

- **Eth** : réseau Grid, réseau Admin ou réseau client.
- **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
- **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau d'administration StorageGRID (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

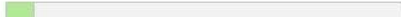
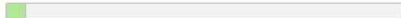
Node information [?](#)

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

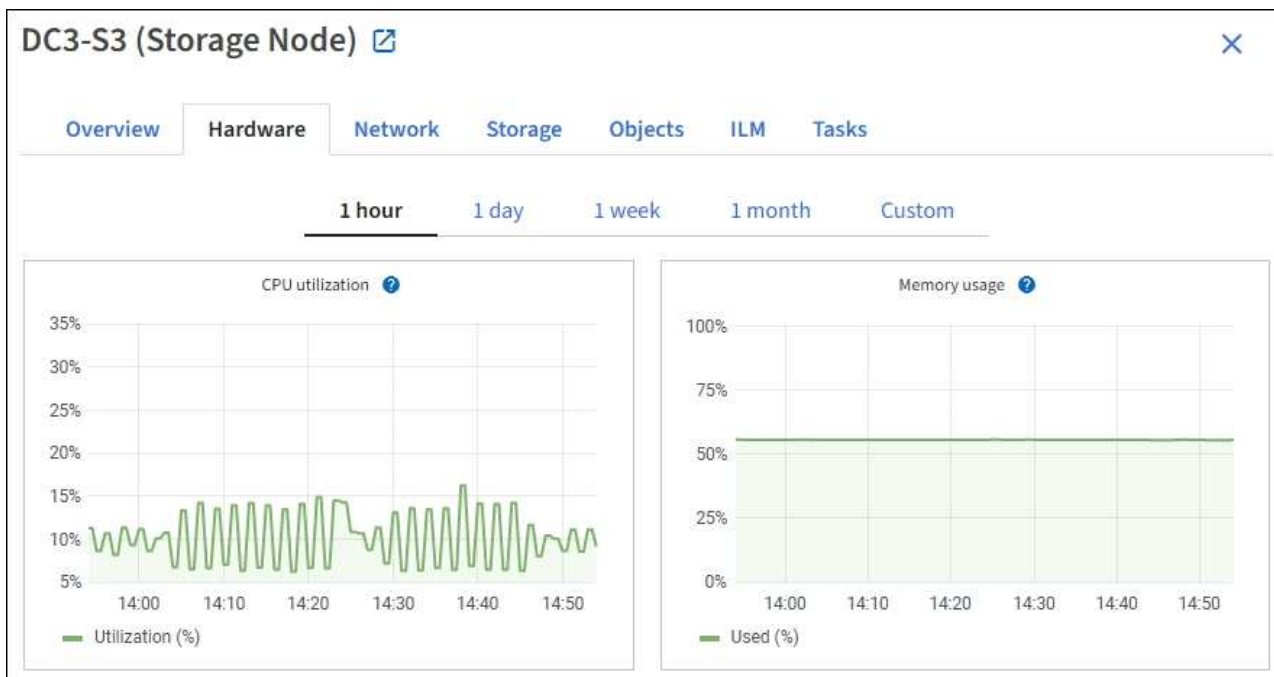
Alerts

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 Overview affiche toutes les alertes actives du nœud.

3. Sélectionnez **matériel** pour plus d'informations sur l'appareil.

- Consultez les graphiques d'utilisation du processeur et de la mémoire pour connaître les pourcentages d'utilisation du processeur et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes situées au-dessus du graphique. Vous pouvez afficher les informations pour des intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, ce 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 le contrôleur de calcul BMC IP et le matériel de calcul, apparaissent uniquement pour les appliances dotées de cette fonctionnalité.

Les composants des tiroirs de stockage et des tiroirs d'extension s'ils font partie de l'installation apparaissent dans un tableau séparé sous le tableau de l'appliance.

Dans la table Appliance	Description
Modèle de type appliance	Le numéro de modèle de cette appliance StorageGRID est indiqué dans SANtricity OS.
Nom du contrôleur de stockage	Nom de cette appliance StorageGRID représenté dans SANtricity OS.
IP de gestion A du contrôleur de stockage	Adresse IP du port de gestion 1 du contrôleur de stockage A. cette adresse IP vous permet d'accéder à SANtricity OS pour résoudre les problèmes de stockage.
IP de gestion du contrôleur de stockage B	Adresse IP du port de gestion 1 du contrôleur de stockage B. cette adresse IP vous permet d'accéder à SANtricity OS pour résoudre les problèmes de stockage. Certains modèles d'appliance ne disposent pas de contrôleur de stockage B.
WWID du contrôleur de stockage	Identifiant universel du contrôleur de stockage indiqué dans SANtricity OS.

Dans la table Appliance	Description
Numéro de série du châssis de l'appliance de stockage	Numéro de série du châssis de l'appareil.
Version du firmware du contrôleur de stockage	Version du firmware du contrôleur de stockage de cette appliance.
Version du contrôleur de stockage SANtricity OS	Version SANtricity OS du contrôleur de stockage A.
Version NVSRAM du contrôleur de stockage	Version NVSRAM du contrôleur de stockage telle que signalée par le Gestionnaire système SANtricity. Pour les SG6060 et SG6160, si la version de NVSRAM ne correspond pas 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	État global du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état de nécessite une intervention pour le matériel de stockage, le système StorageGRID signale également cette valeur. Si l'état est « nécessite une intervention », vérifiez d'abord le contrôleur de stockage à l'aide de SANtricity OS. Ensuite, assurez-vous qu'il n'existe aucune autre alerte qui s'applique au contrôleur de calcul.
Nombre de disques défaillants du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Contrôleur de stockage A	L'état du contrôleur de stockage A.
Contrôleur de stockage B	État du contrôleur de stockage B. certains modèles d'appliance ne disposent pas d'un contrôleur de stockage B.
Alimentation A du contrôleur de stockage	L'état de l'alimentation A du contrôleur de stockage.
Alimentation B du contrôleur de stockage	L'état de l'alimentation B du contrôleur de stockage.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'appliance.

Dans la table Appliance	Description
Taille du disque de stockage des données	La taille effective d'un lecteur de données. Pour le SG6160, la taille du disque cache s'affiche également. Remarque : pour les nœuds avec tiroirs d'extension, utilisez plutôt le Taille de disque des données pour chaque tiroir. La taille effective du disque peut varier en fonction du tiroir.
Mode de stockage RAID	Mode RAID configuré pour l'appliance.
Connectivité du stockage	État de la connectivité du stockage.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de contrôleur BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne disposent pas de matériel de calcul et de stockage distinct.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.
Alimentation du contrôleur de calcul A	État de l'alimentation A du contrôleur de calcul.
Alimentation du contrôleur de calcul B	État de l'alimentation B du contrôleur de calcul.

+

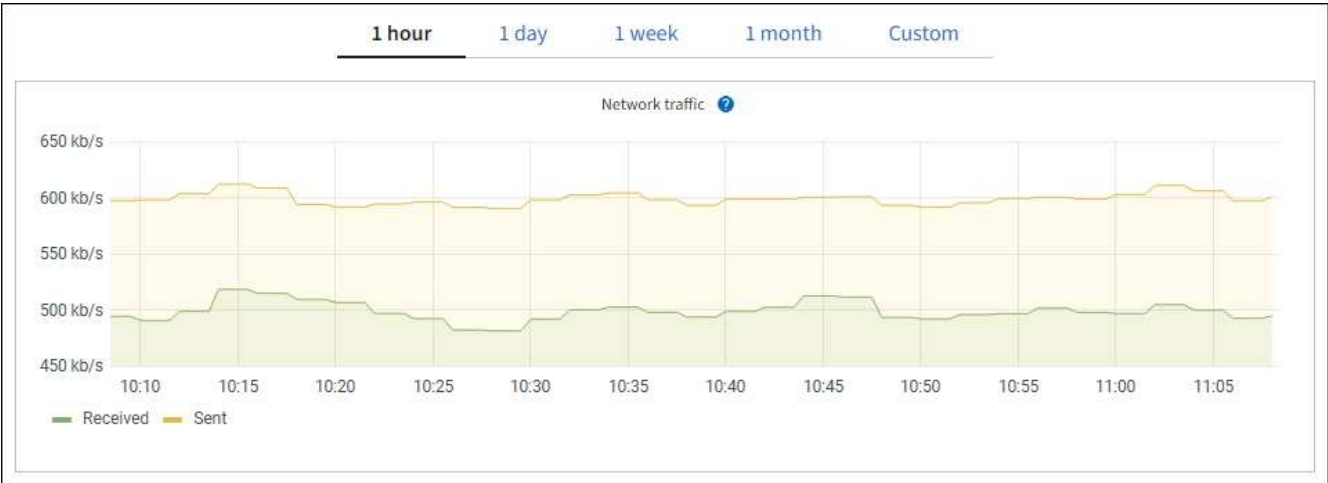
Dans le tableau tiroirs de stockage	Description
Numéro de série du châssis du tiroir	Numéro de série du châssis du tiroir de stockage.
ID du tiroir	Identificateur numérique du tiroir de stockage. • 99 : tiroir contrôleur de stockage • 0 : premier tiroir d'extension • 1 : second tiroir d'extension Remarque : les étagères d'extension s'appliquent uniquement aux SG6060 et SG6160.
État du tiroir	État global du shelf de stockage.
État du module d'E/S.	L'état des modules d'entrée/sortie (IOM) de tous les tiroirs d'extension. S/O s'il ne s'agit pas d'un tiroir d'extension.
État de l'alimentation électrique	État global des alimentations du tiroir de stockage.
État du tiroir	L'état des tiroirs dans le tiroir de rangement. N/A si la tablette ne contient pas de tiroirs.
État du ventilateur	État général des ventilateurs dans le shelf de stockage.
Emplacements de lecteur	Nombre total de slots de disque dans le shelf de stockage.
Disques de données	Nombre de disques du tiroir de stockage utilisés pour le stockage de données.
taille du lecteur de données	Taille effective d'un disque de données dans le tiroir de stockage.
Disques en cache	Nombre de disques du tiroir de stockage utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans le tiroir de stockage. En principe, les disques en cache sont de la même taille.
État de la configuration	L'état de configuration du tiroir de stockage.

a. Confirmer que tous les États sont « nominal ».

Si un état n'est pas « nominal », passez en revue les alertes actuelles. Vous pouvez également utiliser SANtricity System Manager pour en savoir plus sur certaines de ces valeurs matérielles. Reportez-vous aux instructions d'installation et d'entretien de votre appareil.

4. Sélectionnez **réseau** pour afficher les informations de chaque réseau.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section Interfaces réseau.

Network interfaces					
Name ?	Hardware address ?	Speed ?	Duplex ?	Auto-negotiation ?	Link status ?
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Utilisez le tableau suivant avec les valeurs de la colonne **Vitesse** du tableau des 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 du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	25	100
Fixe	LACP	25	50
Fixe	Actif/sauvegarde	25	25
Agrégat	LACP	10	40
Fixe	LACP	10	20
Fixe	Actif/sauvegarde	10	10

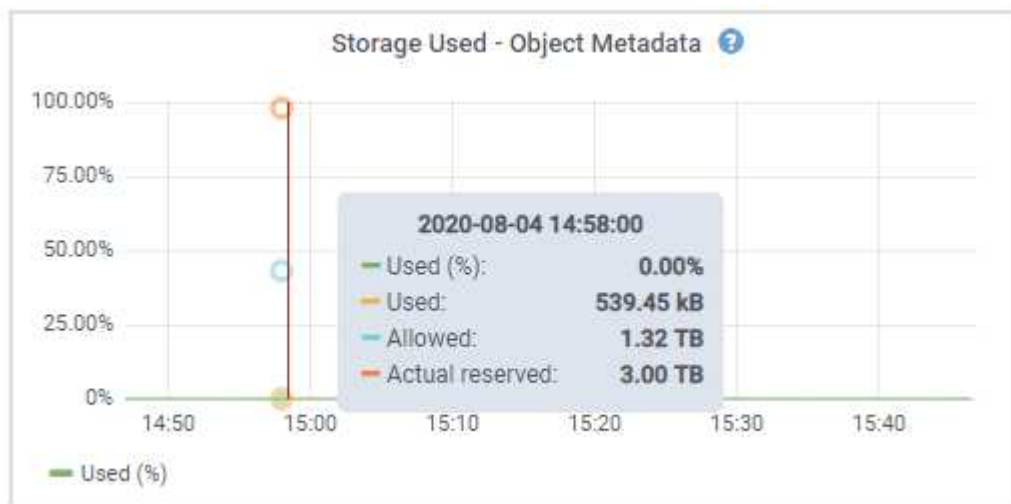
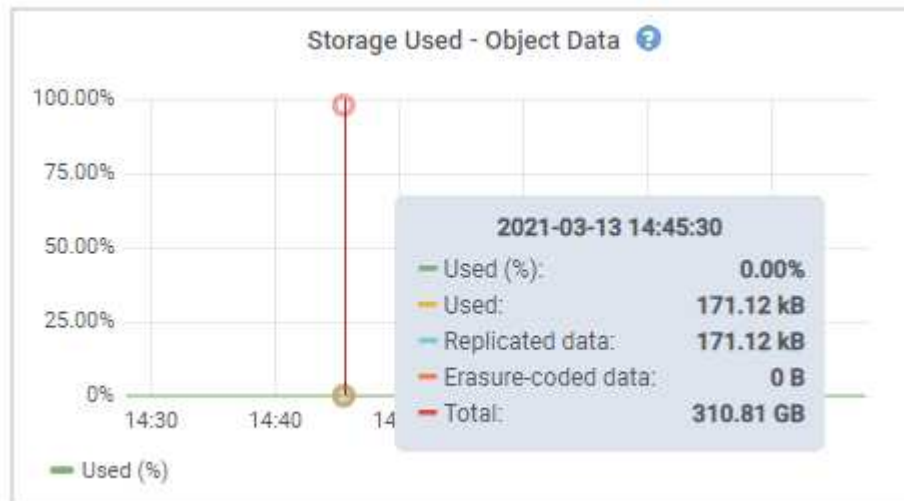
+
Pour plus d’informations sur la configuration des ports 10/25-GbE, reportez-vous à la section "[Configurer](#)"

les liaisons réseau".

- a. Consultez la section sur la communication réseau.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.

5. Sélectionnez **Storage** pour afficher les graphiques qui affichent les pourcentages de stockage utilisés dans le temps pour les données d'objet et les métadonnées d'objet, ainsi que des informations sur les unités de disque, les volumes et les magasins d'objets.



- a. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

Le nom mondial de chaque disque correspond à l'identifiant universel (WWID) du volume qui s'affiche lorsque vous affichez les propriétés standard du volume dans SANtricity OS (le logiciel de gestion connecté au contrôleur de stockage de l'appliance).

Pour vous aider à interpréter les statistiques de lecture et d'écriture du disque relatives aux points de montage du volume, la première partie du nom affichée dans la colonne **Name** de la table Disk Devices (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur indiquée dans la colonne **Device** de la table volumes.

Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle

La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque appliance de services utilisée comme nœud d'administration ou comme nœud de passerelle. Vous pouvez également afficher la mémoire, le matériel de stockage, les ressources réseau, les interfaces réseau, les adresses réseau, et recevoir et transmettre des données.

Étapes

1. Sur la page nœuds, sélectionnez un nœud d'administration d'appliance ou un nœud de passerelle d'appliance.
2. Sélectionnez l'onglet **Aperçu**.

La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :

- **Adllb** et **adlli** : affiché si la liaison actif/sauvegarde est utilisée pour l'interface réseau d'administration
- **Eth** : réseau Grid, réseau Admin ou réseau client.
- **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
- **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau Admin (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

10-224-6-199-ADM1 (Primary Admin Node)

Overview
Hardware
Network
Storage
Load balancer
Tasks
SANtricity System Manager

Node information

Name:
10-224-6-199-ADM1

Type:
Primary Admin Node

ID:
6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:
Connected

Software version:
11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

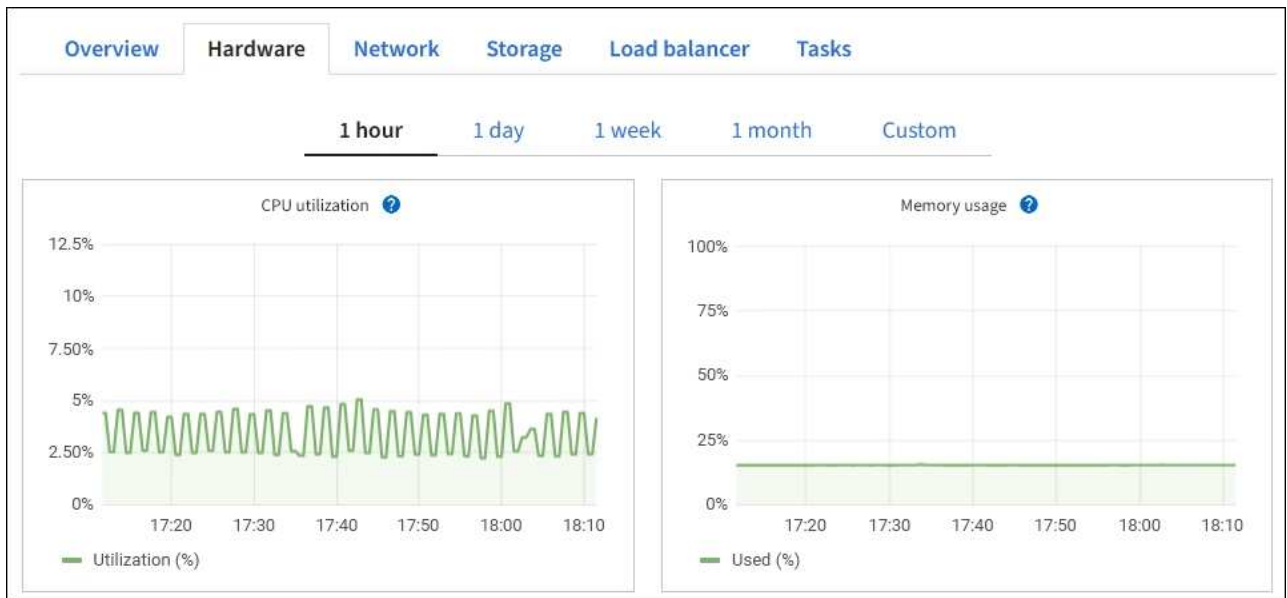
172.16.6.199 - eth0 (Grid Network)
10.224.6.199 - eth1 (Admin Network)
47.47.7.241 - eth2 (Client Network)

Hide additional IP addresses

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

La section alertes de l'onglet Overview affiche toutes les alertes actives du nœud.

3. Sélectionnez l'onglet **Matériel** pour obtenir plus d'informations sur l'appareil.
 - a. Affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.



- b. Faites défiler vers le bas pour consulter le tableau des composants de l'appareil. Ce tableau contient des informations telles que le nom du modèle, le numéro de série, la version du micrologiciel du contrôleur et l'état de chaque composant.

Dans la table Appliance	Description
Modèle de type appliance	Numéro de modèle de cette appliance StorageGRID.
Nombre de disques défaillants du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'apppliance.
Taille du disque de stockage des données	La taille effective d'un lecteur de données.
Mode de stockage RAID	Mode RAID de l'appareil.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'apppliance. Ce champ ne s'affiche pas pour les modèles d'apppliance qui ne contiennent pas de contrôleur BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.

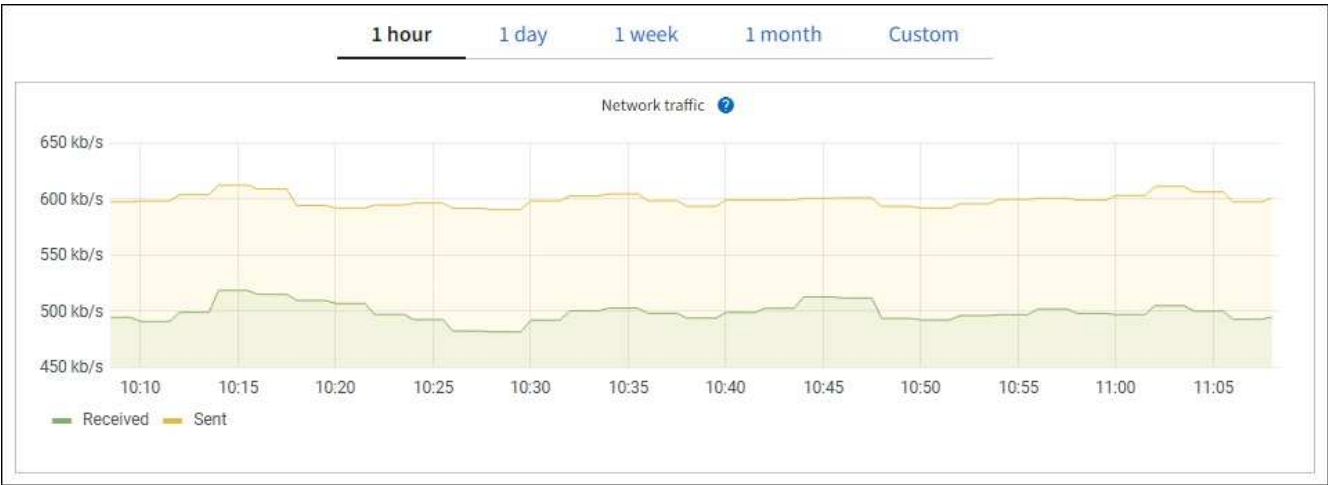
Dans la table Appliance	Description
Matériel de calcul	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

c. Confirmer que tous les États sont « nominal ».

Si un état n'est pas « nominal », passez en revue les alertes actuelles.

4. Sélectionnez l'onglet **Réseau** pour afficher les informations de chaque réseau.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section Interfaces réseau.

Utilisez le tableau suivant avec les valeurs de la colonne **Vitesse** du tableau des interfaces réseau pour déterminer si les quatre ports réseau 40/100-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 du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	100	400
Fixe	LACP	100	200
Fixe	Actif/sauvegarde	100	100

Mode de liaison	Mode du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	40	160
Fixe	LACP	40	80
Fixe	Actif/sauvegarde	40	40

a. Consultez la section sur la 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.

- Sélectionnez l'onglet **Stockage** pour afficher les informations relatives aux périphériques de disque et aux volumes de l'appliance de services.

Affichez l'onglet Réseau StorageGRID

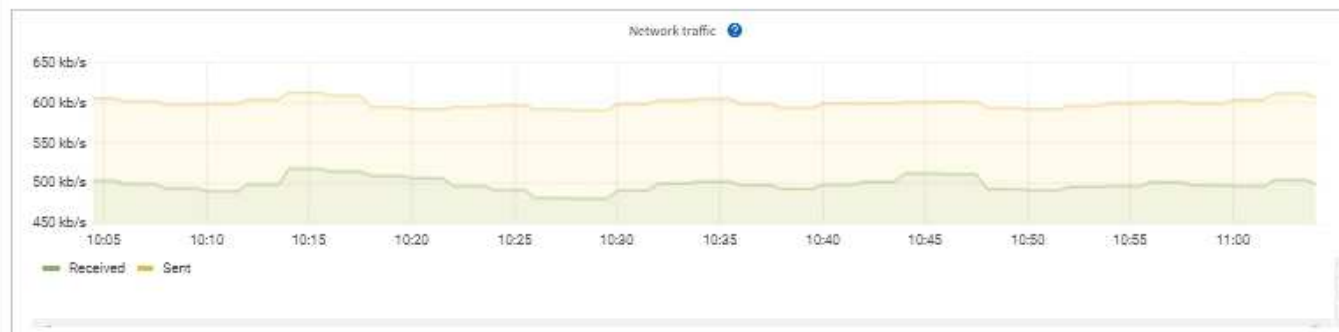
L'onglet réseau affiche un graphique indiquant le trafic réseau reçu et envoyé sur toutes les interfaces réseau du nœud, du site ou de la grille.

L'onglet réseau s'affiche pour tous les nœuds, chaque site et la grille entière.

Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour les nœuds, le tableau interfaces réseau fournit des informations sur les ports réseau physiques de chaque nœud. Le tableau des communications réseau fournit des détails sur les opérations de réception et de transmission de chaque nœud et sur tout compteur d'erreurs signalé par le pilote.

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 associées

"Contrôle des connexions réseau et des performances"

Affichez l'onglet Stockage StorageGRID

L'onglet stockage récapitule la disponibilité du stockage et d'autres mesures de stockage.

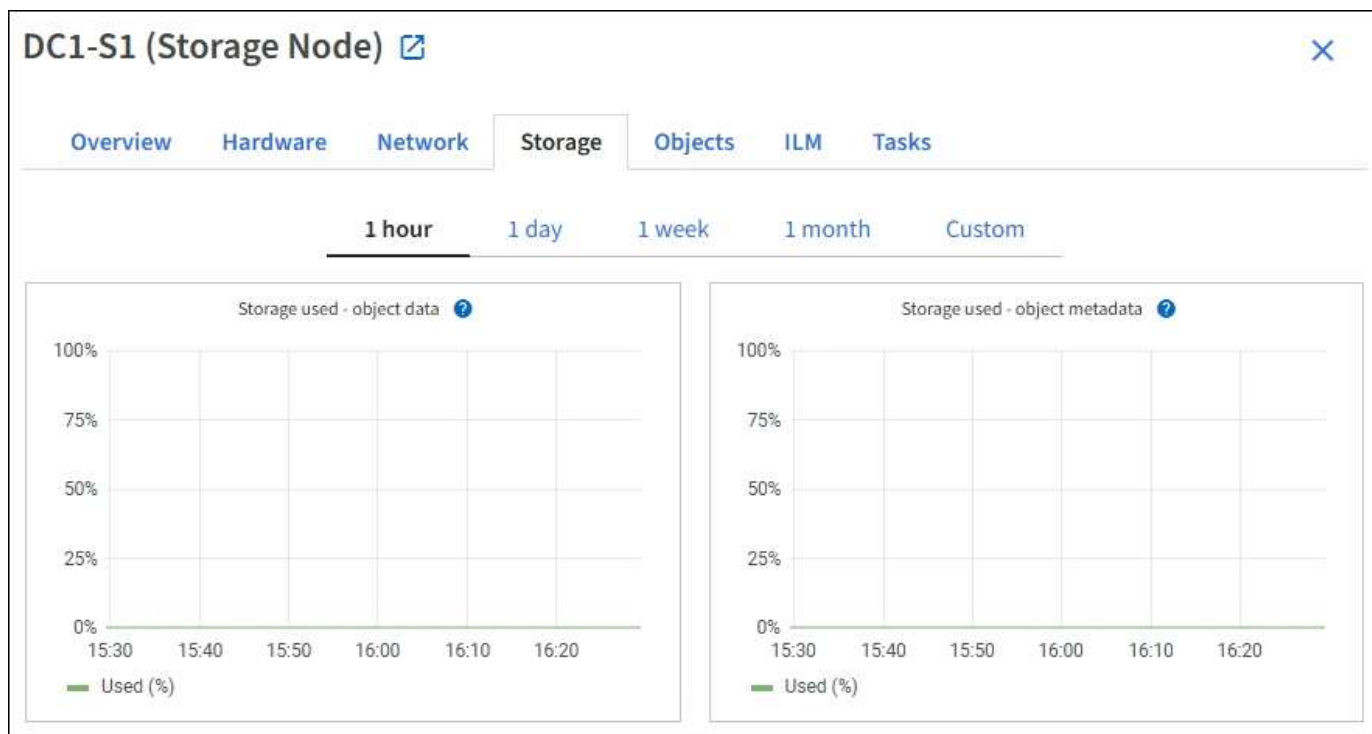
L'onglet Stockage s'affiche pour tous les nœuds, chaque site et l'ensemble de la grille. Cet onglet contient les informations suivantes :

Graphiques utilisés pour le stockage

Pour les nœuds de stockage, chaque site et la grille dans son intégralité, l'onglet stockage contient des graphiques indiquant la quantité de stockage utilisée par les données d'objet et les métadonnées d'objet au fil du temps.



Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.



Tables de stockage des périphériques de disque, des volumes et des objets

Pour tous les nœuds, l'onglet stockage contient des détails sur les unités de disque et les volumes du nœud. Pour les nœuds de stockage, le tableau magasins d'objets fournit des informations sur chaque volume de stockage.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informations associées

["Surveiller la capacité de stockage"](#)

Affichez l'onglet Objets StorageGRID

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

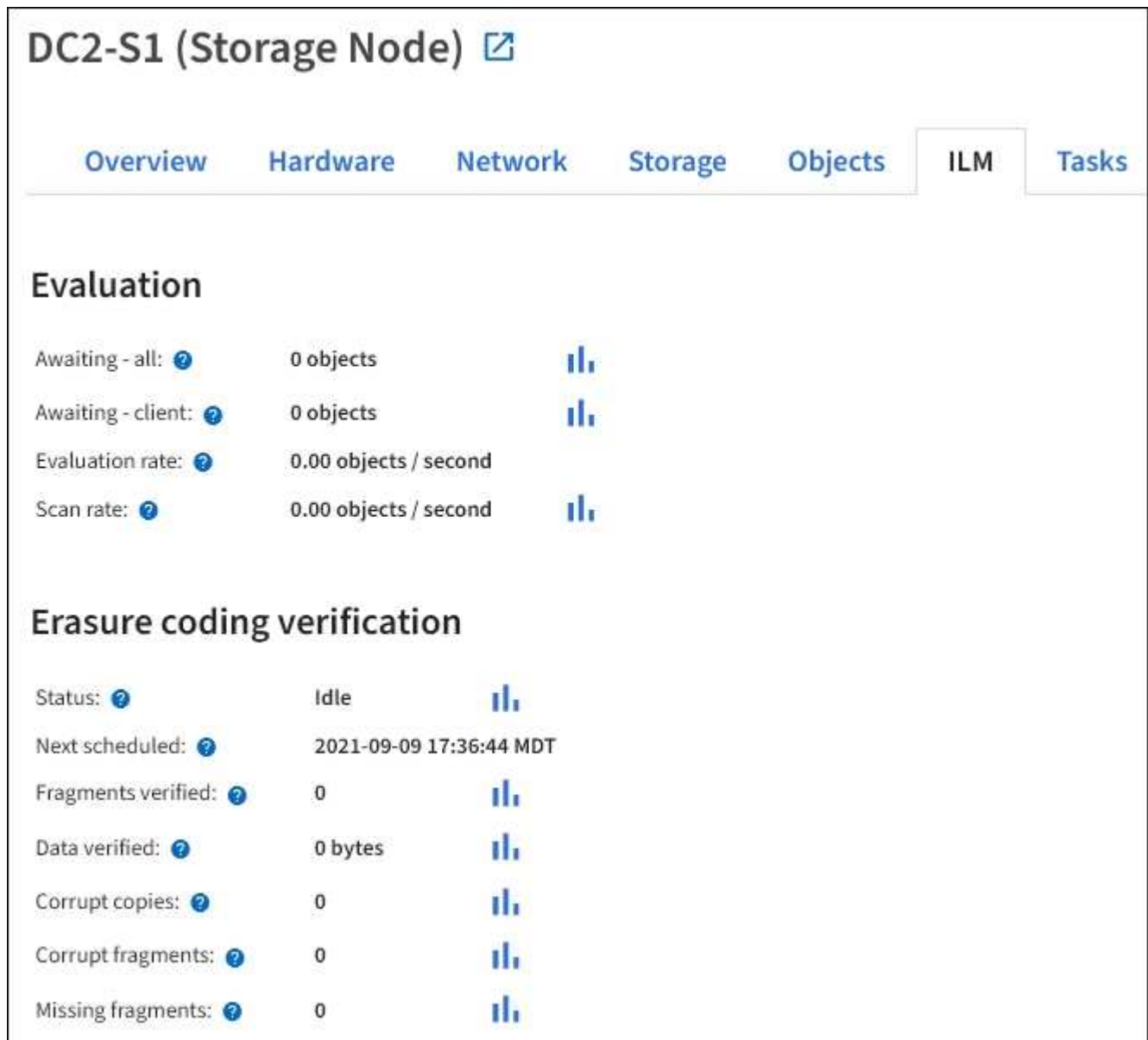
Quarantined objects: ? 0

Affichez l'onglet StorageGRID ILM

L'onglet ILM fournit des informations sur les opérations de gestion du cycle de vie de l'information (ILM).

L'onglet ILM s'affiche pour chaque nœud de stockage, chaque site et la grille dans son ensemble. L'onglet ILM affiche un graphique de la file d'attente ILM sur la durée. Pour la grille, cet onglet indique également le temps estimé de l'analyse ILM complète de tous les objets.

Pour les nœuds de stockage, l'onglet ILM fournit des informations détaillées sur l'évaluation et la vérification en arrière-plan des objets avec code d'effacement.



Informations associées

- ["Contrôle la gestion du cycle de vie des informations"](#)
- ["Administrer StorageGRID"](#)

Utilisez l'onglet Tâches StorageGRID

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 les nœuds de stockage, vous pouvez définir l'état de stockage.

Pour connaître l'ensemble des exigences et des instructions relatives à chaque option de cet onglet, reportez-vous aux sections suivantes :

- ["Renommez la grille, les sites et les nœuds"](#)
- ["Redémarrez le nœud de la grille"](#)
- ["Mettez l'appareil en mode maintenance"](#)
- Vous vérifiez ou définissez l'état de stockage d'un nœud de stockage après avoir ajouté des volumes à connexion directe ou SAN au nœud de stockage, ou après avoir récupéré un nœud de stockage. Ces instructions sont disponibles dans les rubriques qui décrivent ces tâches.

Affichez l'onglet Équilibreur de charge StorageGRID

L'onglet Load Balancer contient des graphiques de performance et de diagnostic relatifs au fonctionnement du service Load Balancer.

L'onglet Load Balancer s'affiche pour les nœuds d'administration et les nœuds de passerelle, chaque site et la grille dans son ensemble. Pour chaque site, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les nœuds de ce site. Pour toute la grille, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les sites.

Si aucune E/S n'est exécutée via le service Load Balancer ou si aucun équilibreur de charge n'est configuré, les graphiques affichent « aucune donnée ».



Trafic des demandes

Ce graphique fournit une moyenne mobile de 3 minutes du débit des données transmises entre les terminaux de l'équilibreur de charge et les clients effectuant les demandes, en bits par seconde.



Cette valeur est mise à jour à la fin de chaque demande. Par conséquent, cette valeur peut différer du débit en temps réel à des taux de demande faibles ou pour des demandes très longues. Vous pouvez consulter l'onglet réseau pour obtenir une vue plus réaliste du comportement actuel du réseau.

Taux de demande entrante

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de nouvelles demandes par seconde, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle demande ont été validés.

Durée moyenne de la demande (non-erreur)

Ce graphique fournit une moyenne mobile de 3 minutes des durées de requête, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Chaque durée de la demande commence lorsqu'un en-tête de requête est analysé par le service Load Balancer et se termine lorsque le corps de réponse complet

est renvoyé au client.

Taux de réponse à l'erreur

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de réponses d'erreur renvoyées aux clients par seconde, ventilées par le code de réponse d'erreur.

Informations associées

- ["Surveiller les opérations d'équilibrage de charge"](#)
- ["Administrer StorageGRID"](#)

Consultez l'onglet Services de la plateforme StorageGRID

L'onglet Services de plateforme fournit des informations sur les opérations de service de la plateforme S3 sur un site.

L'onglet Platform Services s'affiche pour chaque site. Cet onglet fournit des informations sur les services de la plateforme S3, comme la réplication CloudMirror et le service d'intégration de la recherche. Les graphiques de cet onglet affichent des mesures telles que le nombre de requêtes en attente, le taux d'achèvement de la requête et le taux d'échec de la requête.

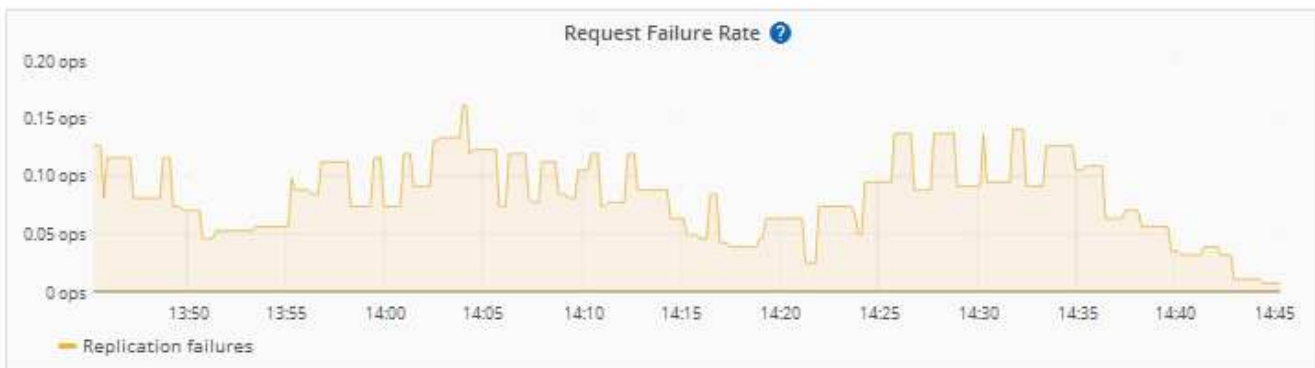
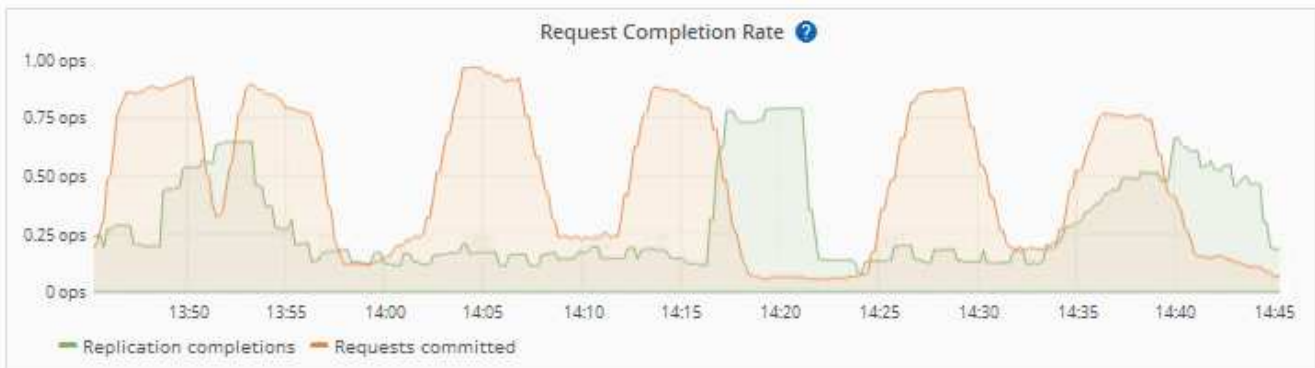
1 hour

1 day

1 week

1 month

Custom



Pour plus d'informations sur les services de plateforme S3, notamment des détails de dépannage, consultez le ["Instructions d'administration de StorageGRID"](#).

Consultez l'onglet Gérer les disques de StorageGRID

L'onglet gérer les disques vous permet d'accéder aux détails et d'effectuer des tâches de dépannage et de maintenance sur les disques des appliances qui prennent en charge cette fonctionnalité.

L'onglet gérer les lecteurs vous permet d'effectuer les opérations suivantes :

- Afficher la disposition des disques de stockage des données du système
- Affichez un tableau répertoriant l'emplacement, le type, l'état, la version du micrologiciel et le numéro de série de chaque lecteur
- Exécutez les fonctions de dépannage et de maintenance sur chaque disque

Pour accéder à l'onglet gérer les lecteurs, vous devez disposer du ["Administrateur de l'appliance de stockage ou autorisation d'accès racine"](#).

Pour plus d'informations sur l'utilisation de l'onglet gérer les lecteurs, reportez-vous à la section ["Utilisez l'onglet gérer les lecteurs"](#).

Affichez l'onglet SANtricity System Manager de StorageGRID

L'onglet SANtricity System Manager vous permet d'accéder à SANtricity System Manager sans devoir configurer ni connecter le port de gestion de l'appliance de stockage. Cet onglet permet de consulter les informations de diagnostic du matériel et les informations environnementales, ainsi que les problèmes liés aux lecteurs.



L'accès à SANtricity System Manager à partir de Grid Manager se limite généralement à la surveillance du matériel de l'appliance et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de l'appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions de maintenance du matériel de votre appareil. Pour mettre à niveau le micrologiciel SANtricity, reportez-vous au ["Procédures de configuration de la maintenance"](#) pour votre appliance de stockage.



L'onglet SANtricity System Manager s'affiche uniquement pour les nœuds d'appliance de stockage qui utilisent le matériel E-Series.

Grâce à SANtricity System Manager, vous pouvez effectuer les opérations suivantes :

- Affichez des données sur les performances, telles que les performances au niveau des baies de stockage, la latence des E/S, l'utilisation du CPU du contrôleur de stockage et le débit.
- Vérifiez l'état des composants matériels.
- Exécutez des fonctions de support, notamment l'affichage des données de diagnostic et la configuration du système E-Series AutoSupport.



Pour utiliser SANtricity System Manager afin de configurer un proxy pour E-Series AutoSupport, consultez ["Envoyez des packages AutoSupport E-Series via StorageGRID"](#).

Pour accéder au Gestionnaire système SANtricity via le Gestionnaire de grille, vous devez disposer du ["Administrateur de l'appliance de stockage ou autorisation d'accès racine"](#).



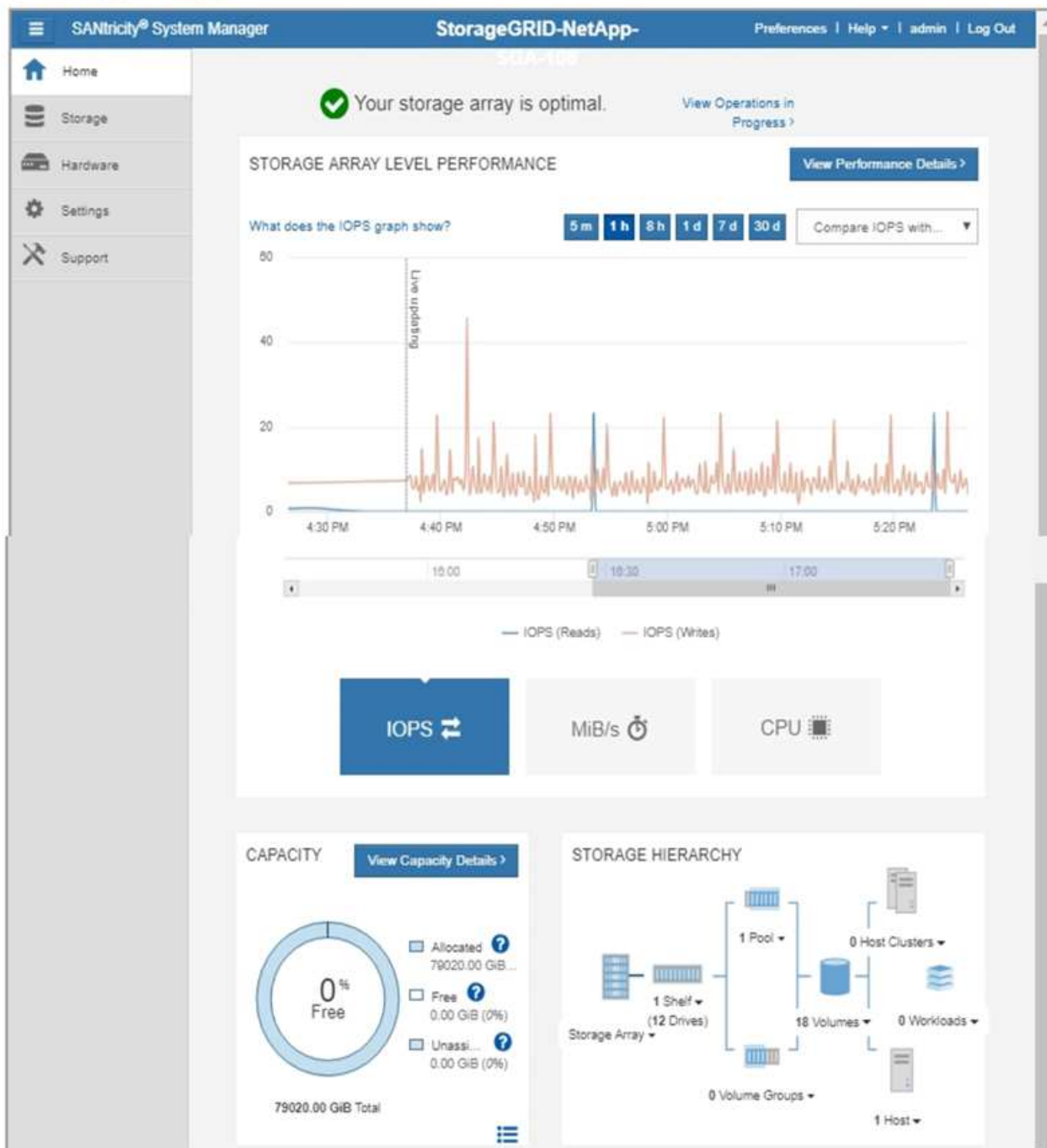
Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

L'onglet affiche la page d'accueil de SANtricity System Manager.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



Pour plus de facilité, vous pouvez utiliser le lien SANtricity System Manager pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur.

Pour afficher des informations détaillées sur les performances au niveau de la baie de stockage et l'utilisation

de la capacité, positionnez le curseur sur chaque graphique.

Pour plus d'informations sur l'affichage des informations accessibles depuis l'onglet Gestionnaire système SANtricity, reportez-vous à la section "[Documentation sur les systèmes NetApp E-Series et SANtricity](#)".

Informations à surveiller régulièrement

Que surveiller et quand dans StorageGRID

Même si le système StorageGRID peut continuer à fonctionner lorsque des erreurs se produisent ou que des parties de la grille sont indisponibles, vous devez surveiller et résoudre les problèmes potentiels avant qu'ils n'affectent l'efficacité ou la disponibilité de la grille.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

A propos des tâches de surveillance

Un système occupé génère de grandes quantités d'informations. La liste suivante fournit des conseils sur les informations les plus importantes à surveiller en permanence.

Quoi surveiller	Fréquence
" État de santé du système "	Tous les jours
Taux de " Capacité des objets et des métadonnées du nœud de stockage " consommation	Hebdomadaire
" Opérations de gestion du cycle de vie des informations "	Hebdomadaire
" Ressources réseau et système "	Hebdomadaire
" Activité des locataires "	Hebdomadaire
" Opérations client S3 "	Hebdomadaire
" Opérations d'équilibrage de la charge "	Après la configuration initiale et après toute modification de la configuration
" Connexions de fédération de grille "	Hebdomadaire

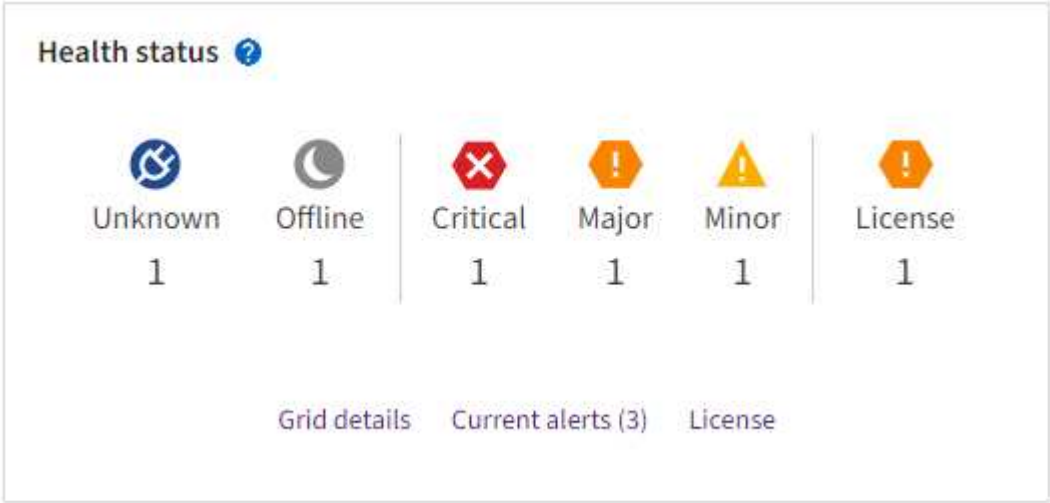
Surveillez l'état du système dans StorageGRID

Surveillez quotidiennement l'état global de votre système StorageGRID.

Description de la tâche

Le système StorageGRID peut continuer à fonctionner lorsque certaines parties de la grille ne sont pas disponibles. Les problèmes potentiels signalés par des alertes ne sont pas nécessairement des problèmes liés aux opérations du système. Examinez les problèmes résumés sur la carte d'état de santé du tableau de bord Grid Manager.

Pour être averti des alertes dès qu'elles sont déclenchées, vous pouvez ["configurez les notifications par e-mail pour les alertes"](#) ou ["Configurer les interruptions SNMP"](#).



Lorsque des problèmes existent, des liens s'affichent pour vous permettre d'afficher des détails supplémentaires :

Lien	Apparaît lorsque...
Détails de la grille	Tous les nœuds sont déconnectés (état de connexion inconnu ou arrêté administrativement).
Alertes actuelles (critique, majeure, mineure)	Les alertes sont actuellement actif .
Alertes récemment résolues	Alertes déclenchées au cours de sont maintenant résolus la semaine dernière .
Licence	Il y a un problème avec la licence logicielle de ce système StorageGRID. Vous pouvez "mettez à jour les informations de licence si nécessaire" .

Surveiller les États de connexion du nœud

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations StorageGRID stratégiques peuvent être affectées. Surveillez les États de connexion des nœuds et traitez tous les problèmes rapidement.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue. L'alerte Impossible de communiquer avec le nœud peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. Sélectionnez chaque alerte et suivre les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud. Remarque : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.
	Non connecté - Arrêt administratif Pour une raison prévue, le nœud n'est pas connecté au grid. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives sélectionnez chaque alerte et suivez les actions recommandées.
	• Connecté* Le nœud est connecté à la grille.	Aucune action requise.

Afficher les alertes actuelles et résolues

Alertes actuelles : lorsqu'une alerte est déclenchée, une icône d'alerte s'affiche sur le tableau de bord. Une icône d'alerte s'affiche également pour le nœud sur la page nœuds. Si "[les notifications par e-mail d'alerte sont configurées](#)", une notification par e-mail sera également envoyée, sauf si l'alerte a été neutralisée.

Alertes résolues : vous pouvez rechercher et afficher un historique des alertes qui ont été résolues.

En option, vous avez regardé la vidéo :

[Aperçu des alertes](#)

Le tableau suivant décrit les informations affichées dans Grid Manager pour les alertes en cours et résolues.

En-tête de colonne	Description
Nom ou titre	Le nom de l'alerte et sa description.
Gravité	Gravité de l'alerte. Pour les alertes actuelles, si plusieurs alertes sont regroupées, la ligne de titre indique le nombre d'instances de cette alerte qui se produisent à chaque gravité.  Critique : Une condition anormale existe qui a interrompu le fonctionnement normal d'un nœud ou service StorageGRID. Vous devez résoudre immédiatement le problème sous-jacent. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu.  Majeur : Une anomalie existe qui affecte les opérations en cours ou approche le seuil d'alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tout problème sous-jacent afin de garantir que l'anomalie ne perturbe pas le fonctionnement normal d'un nœud ou service StorageGRID.  Mineur : Le système fonctionne normalement, mais une anomalie existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne se résolvent pas d'elles-mêmes afin de vous assurer qu'elles ne provoquent pas un problème plus grave.
Temps déclenché	Alertes actuelles : date et heure auxquelles l'alerte a été déclenchée à l'heure locale et en UTC. Si plusieurs alertes sont regroupées, la ligne de titre affiche les heures de l'instance la plus récente de l'alerte (<i>le plus récent</i>) et de l'instance la plus ancienne de l'alerte (<i>le plus ancien</i>). Alertes résolues : il y a combien de temps l'alerte a été déclenchée.
Site/nœud	Nom du site et du nœud où l'alerte a eu lieu ou s'est produite.
État	Indique si l'alerte est active, neutralisée ou résolue. Si plusieurs alertes sont regroupées et que toutes les alertes sont sélectionnées dans la liste déroulante, la ligne de titre indique le nombre d'instances de cette alerte actives et le nombre d'instances désactivées.
Temps résolu (alertes résolues uniquement)	Il y a combien de temps l'alerte a été résolue.
Valeurs actuelles ou <i>valeurs de données</i>	Valeur de la mesure à l'origine du déclenchement de l'alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l'alerte. Par exemple, les valeurs affichées pour une alerte stockage de données d'objet bas comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée. Remarque : si plusieurs alertes actuelles sont regroupées, les valeurs actuelles ne sont pas affichées dans la ligne de titre.

En-tête de colonne	Description
Valeurs déclenchées (alertes résolues uniquement)	Valeur de la mesure à l'origine du déclenchement de l'alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l'alerte. Par exemple, les valeurs affichées pour une alerte stockage de données d'objet bas comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée.

Étapes

1. Sélectionnez le lien **alertes actuelles** ou **alertes résolues** pour afficher la liste des alertes de ces catégories. Vous pouvez également afficher les détails d'une alerte en sélectionnant **nœuds > nœud > vue d'ensemble**, puis en sélectionnant l'alerte dans le tableau alertes.

Par défaut, les alertes actuelles s'affichent comme suit :

- Les alertes déclenchées les plus récemment sont affichées en premier.
- Plusieurs alertes du même type sont affichées sous la forme d'un groupe.
- Les alertes qui ont été neutralisées ne sont pas affichées.
- Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un niveau de gravité, seule l'alerte la plus grave est affichée. C'est-à-dire, si les seuils d'alerte sont atteints pour les niveaux de gravité mineur, majeur et critique, seule l'alerte critique s'affiche.

La page d'alertes en cours est actualisée toutes les deux minutes.

2. Pour développer les groupes d'alertes, sélectionnez la flèche vers le bas ▼. Pour réduire les alertes individuelles d'un groupe, sélectionnez la flèche 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 ou groupes d'alertes en cours, sélectionnez les flèches haut/bas ⬆️⬆️ dans l'en-tête de chaque colonne.
 - Lorsque **alertes de groupe** est sélectionné, les groupes d'alertes et les alertes individuelles de chaque groupe sont triés. Par exemple, vous pouvez trier les alertes d'un groupe par **heure déclenchée** pour trouver l'instance la plus récente d'une alerte spécifique.
 - Lorsque **alertes de groupe** est effacé, la liste complète des alertes est triée. Par exemple, vous pouvez trier toutes les alertes par **nœud/site** pour voir toutes les alertes affectant un nœud spécifique.
5. Pour filtrer les alertes actuelles par état (**toutes les alertes**, **Active** ou **Silence**, utilisez le menu déroulant situé en haut du tableau.

Voir "[Notifications d'alerte de silence](#)".

6. Pour trier les alertes résolues :
 - Sélectionnez une période dans le menu déroulant **lorsqu'elle est déclenchée**.
 - Sélectionnez une ou plusieurs gravité dans le menu déroulant **gravité**.
 - Sélectionnez une ou plusieurs règles d'alerte par défaut ou personnalisées dans le menu déroulant **règle d'alerte** pour filtrer les alertes résolues associées à une règle d'alerte spécifique.
 - Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Node** pour filtrer les alertes résolues liées à un nœud spécifique.

7. Pour afficher les détails d'une alerte spécifique, sélectionnez l'alerte. Une boîte de dialogue fournit des détails et des actions recommandées pour l'alerte que vous avez sélectionnée.
8. (Facultatif) pour une alerte spécifique, sélectionnez silence cette alerte pour désactiver la règle d'alerte qui a déclenché cette alerte.

Vous devez avoir le ["Gérer les alertes ou l'autorisation d'accès racine"](#) pour désactiver une règle d'alerte.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

9. Pour afficher les conditions actuelles de la règle d'alerte :

- a. Dans les détails de l'alerte, sélectionnez **Afficher les conditions**.

Une fenêtre contextuelle s'affiche, répertoriant l'expression Prometheus pour chaque gravité définie.

- b. Pour fermer la fenêtre contextuelle, sélectionnez n'importe quel emplacement en dehors de la fenêtre contextuelle.

10. Vous pouvez également sélectionner **Modifier la règle** pour modifier la règle d'alerte qui a déclenché cette alerte.

Vous devez avoir le ["Gérer les alertes ou l'autorisation d'accès racine"](#) pour modifier une règle d'alerte.



Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne détéciez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

11. Pour fermer les détails de l'alerte, sélectionnez **Fermer**.

Surveillez la capacité de stockage dans StorageGRID

Contrôlez l'espace total disponible pour vérifier que le système StorageGRID ne manque pas d'espace de stockage pour les objets ou les métadonnées d'objet.

StorageGRID stocke séparément les données d'objet et les métadonnées d'objet. Il réserve un espace spécifique pour une base de données Cassandra distribuée qui contient les métadonnées d'objet. Surveiller la quantité totale d'espace consommée pour les objets et les métadonnées d'objet, ainsi que les tendances en matière de quantité d'espace consommée pour chaque. Vous pourrez ainsi planifier l'ajout de nœuds et éviter toute panne de service.

Vous pouvez ["affichez des informations sur la capacité de stockage"](#) couvrir l'ensemble de la grille, pour chaque site et pour chaque nœud de stockage du système StorageGRID.

Surveiller la capacité de stockage pour l'ensemble de la grille

Surveillez la capacité de stockage globale de votre grid afin de vous assurer qu'il reste un espace libre adéquat pour les données d'objet et les métadonnées d'objet. Pour mieux comprendre les variations de capacité de stockage dans le temps, vous pouvez planifier l'ajout de nœuds de stockage ou de volumes avant de consommer la capacité de stockage utilisable de la grille.

Le tableau de bord de Grid Manager vous permet d'évaluer rapidement la quantité de stockage disponible pour l'ensemble du grid et pour chaque data Center. La page nœuds fournit des valeurs plus détaillées pour

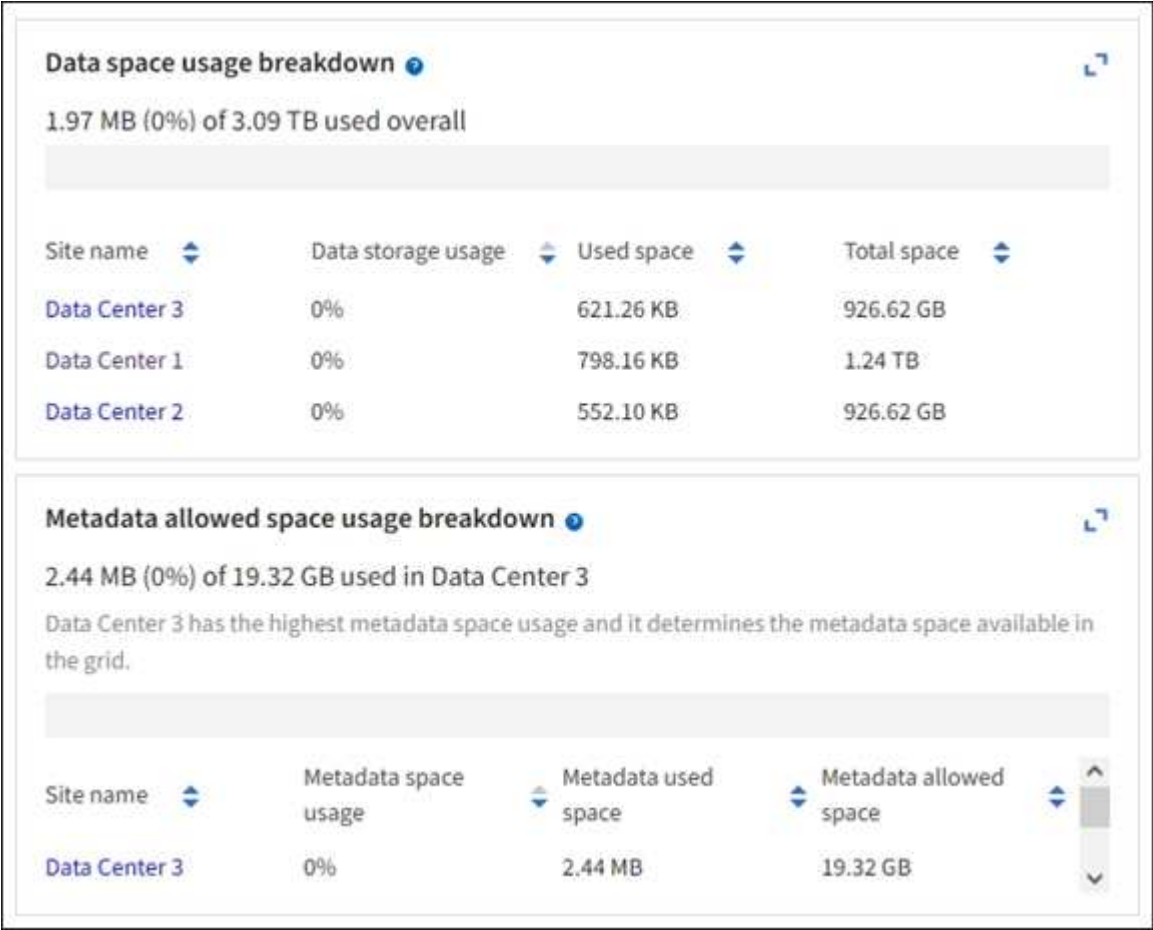
les données d'objet et les métadonnées d'objet.

Étapes

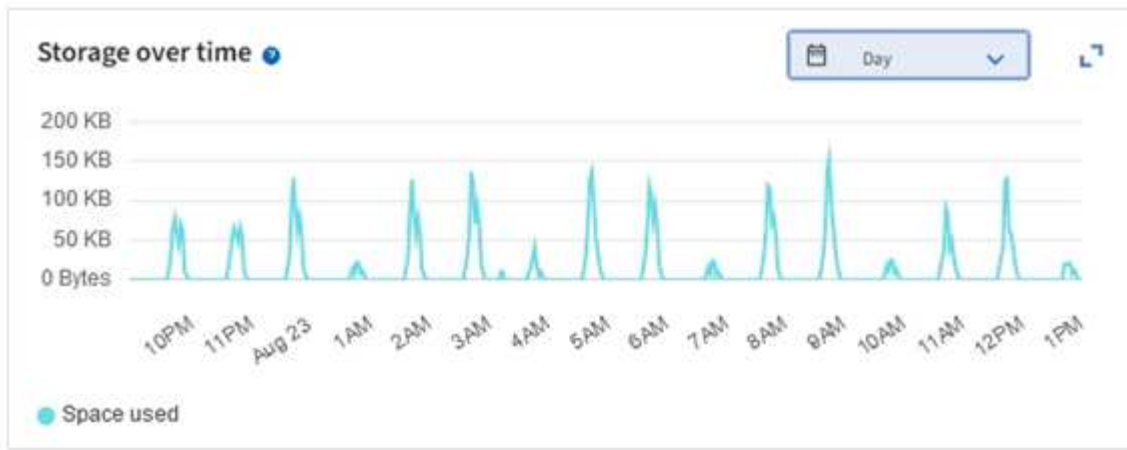
- 1. Évaluez la quantité de stockage disponible pour l'ensemble du grid et pour chaque data Center.
 - a. Sélectionnez **Tableau de bord > vue d'ensemble**.
 - b. Notez les valeurs de la répartition de l'utilisation de l'espace de données et les cartes de répartition de l'utilisation de l'espace autorisé dans les métadonnées. Chaque carte indique un pourcentage d'utilisation du stockage, la capacité de l'espace utilisé et l'espace total disponible ou autorisé par site.



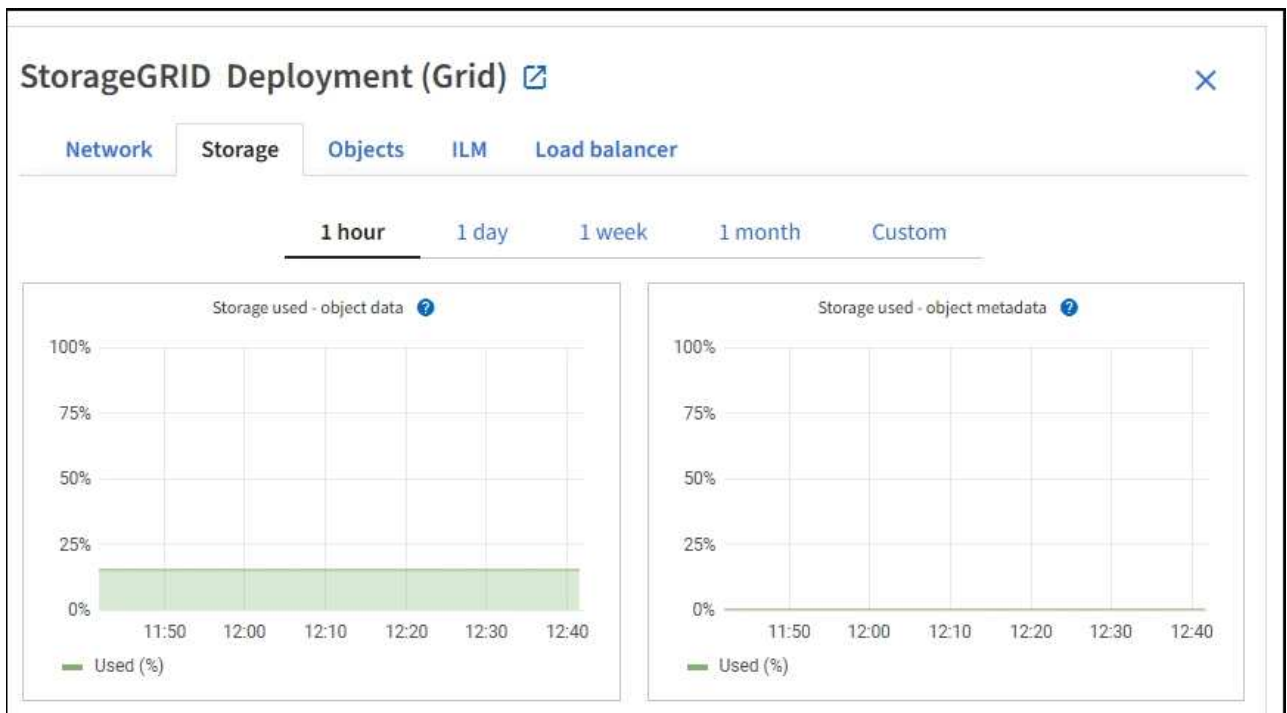
Le résumé n'inclut pas les supports d'archivage.



- a. Notez le tableau sur la carte de stockage dans le temps. Utilisez la liste déroulante période pour vous aider à déterminer la rapidité de consommation du stockage.



2. Pour plus d'informations sur la quantité de stockage utilisée et la quantité de stockage restant disponible dans la grille pour les données d'objet et les métadonnées d'objet, consultez la page nœuds.
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez **GRID > stockage**.



- c. Placez votre curseur sur les graphiques **stockage utilisé - données d'objet** et **stockage utilisé - métadonnées d'objet** pour connaître la quantité de stockage d'objet et de métadonnées d'objet disponible pour l'ensemble de la grille, ainsi que la quantité utilisée au fil du temps.



Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Planifiez une extension permettant d'ajouter des nœuds de stockage ou des volumes de stockage avant l'utilisation de la capacité de stockage utilisable de la grille.

Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.



Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

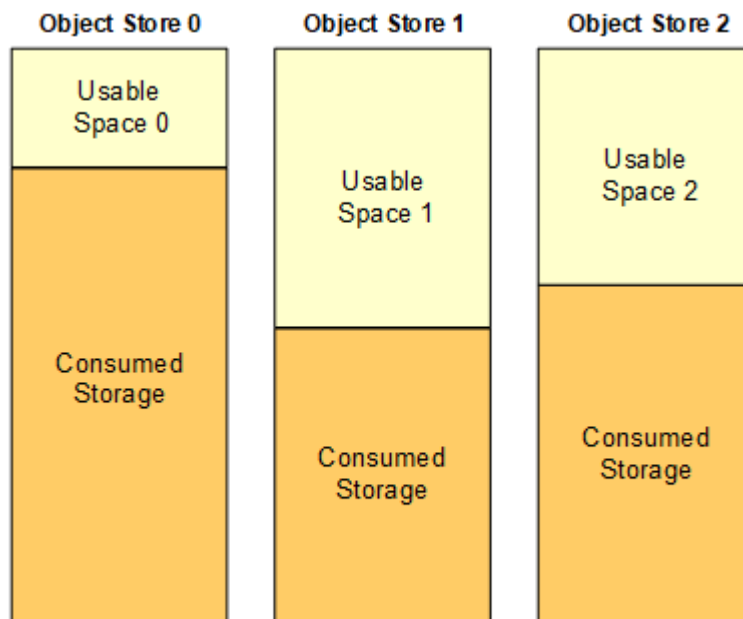
Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au ["Instructions d'extension de StorageGRID"](#).

Surveillez la capacité de stockage de chaque nœud de stockage

Surveillez l'espace total utilisable pour chaque nœud de stockage pour vous assurer que le nœud dispose de suffisamment d'espace pour les nouvelles données d'objet.

Description de la tâche

L'espace utilisable correspond à la quantité d'espace de stockage disponible pour stocker des objets. L'espace total utilisable d'un nœud de stockage est calculé en ajoutant ensemble l'espace disponible sur tous les magasins d'objets du nœud.



$$\text{Total Usable Space} = \text{Usable Space 0} + \text{Usable Space 1} + \text{Usable Space 2}$$

Étapes

1. Sélectionnez **Nœuds > Nœud de stockage > Stockage**.

Les graphiques et les tableaux du nœud apparaissent.

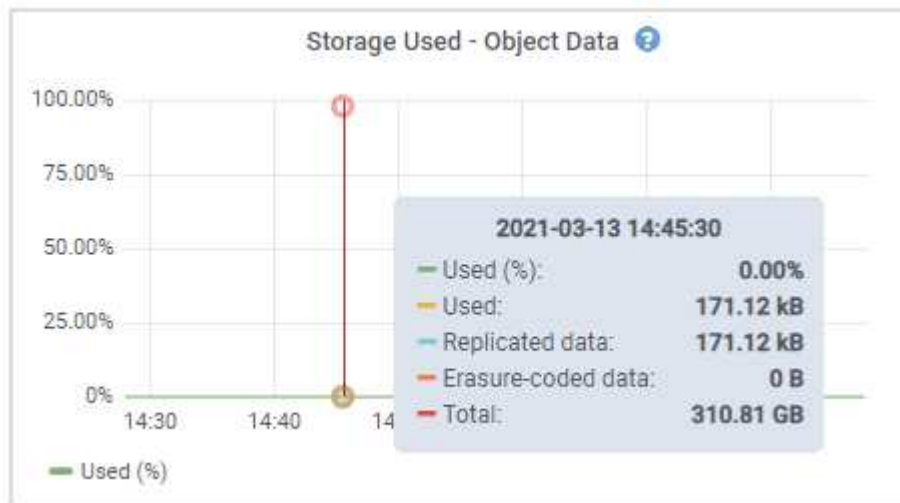
2. Positionnez le curseur sur le graphique de données d'objet stockage utilisé -.

Les valeurs suivantes sont affichées :

- **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
- **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code

d'effacement sur ce nœud, ce site ou ce grid.

- **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` mesure.



3. Passez en revue les valeurs disponibles dans les tableaux volumes et magasins d'objets, sous les graphiques.



Pour visualiser les graphiques de ces valeurs, sélectionnez les icônes de graphique dans les colonnes disponibles.

4. Surveillez les valeurs dans le temps pour estimer le taux de consommation de l'espace de stockage utilisable.
5. Pour préserver le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant de consommer l'espace utilisable.

Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.



Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au ["Instructions d'extension de StorageGRID"](#).

L'"[Faible stockage des données objet](#)" alerte est déclenchée lorsque l'espace restant est insuffisant pour stocker les données d'objet sur un nœud de stockage.

Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage

Surveillez l'utilisation des métadonnées pour chaque nœud de stockage afin de garantir qu'un espace adéquat reste disponible pour les opérations essentielles de la base de données. Vous devez ajouter de nouveaux nœuds de stockage sur chaque site avant que les métadonnées d'objet dépassent 100 % de l'espace autorisé pour les métadonnées.

Description de la tâche

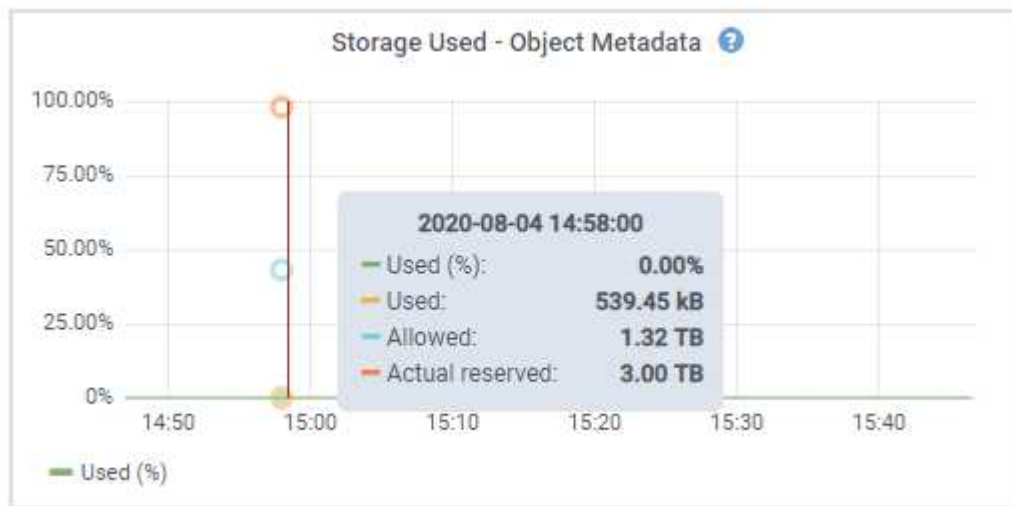
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site, en utilisant l'espace réservé aux métadonnées sur le volume de stockage 0 de chaque nœud de stockage.

Dans certains cas, la capacité des métadonnées d'objet de la grille peut être utilisée plus rapidement que la capacité de stockage objet. Par exemple, si vous ingérez généralement un grand nombre d'objets de petite taille, vous devrez ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage objet est suffisante.

L'utilisation des métadonnées peut notamment être augmentée, comme la taille et la quantité des métadonnées et du balisage, le nombre total d'éléments d'un téléchargement partitionné et la fréquence des modifications apportées aux emplacements de stockage ILM.

Étapes

1. Sélectionnez **Nœuds > Nœud de stockage > Stockage**.
2. Positionnez le curseur sur le graphique de métadonnées de l'objet stockage utilisé - pour afficher les valeurs d'une heure spécifique.



Utilisé (%)

Pourcentage de l'espace de métadonnées autorisé utilisé sur ce nœud de stockage.

Metrics Prometheus : `storagegrid_storage_utilization_metadata_bytes` et `storagegrid_storage_utilization_metadata_allowed_bytes`

Utilisé

Les octets de l'espace de métadonnées autorisé qui ont été utilisés sur ce nœud de stockage.

Prometheus métrique : `storagegrid_storage_utilization_metadata_bytes`

Autorisé

Espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour savoir comment cette valeur est déterminée pour chaque nœud de stockage, reportez-vous au ["Description complète de l'espace de métadonnées autorisé"](#).

Prometheus métrique : `storagegrid_storage_utilization_metadata_allowed_bytes`

Réserve réelle

Espace réel réservé aux métadonnées sur ce nœud de stockage. Inclut l'espace autorisé et l'espace requis pour les opérations essentielles sur les métadonnées. Pour savoir comment cette valeur est calculée pour chaque nœud de stockage, reportez-vous au ["Description complète de l'espace réservé réel pour les métadonnées"](#).

Prometheus métrique sera ajouté dans une prochaine version.



Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Si la valeur **utilisée (%)** est de 70 % ou plus, développez votre système StorageGRID en ajoutant des nœuds de stockage à chaque site.



L'alerte **stockage de métadonnées faible** est déclenchée lorsque la valeur **utilisée (%)** atteint certains seuils. Les résultats indésirables peuvent se produire si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé.

Lorsque vous ajoutez des nœuds, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage du site. Voir la ["Instructions d'extension d'un système StorageGRID"](#).

Surveillez les prévisions d'utilisation de l'espace

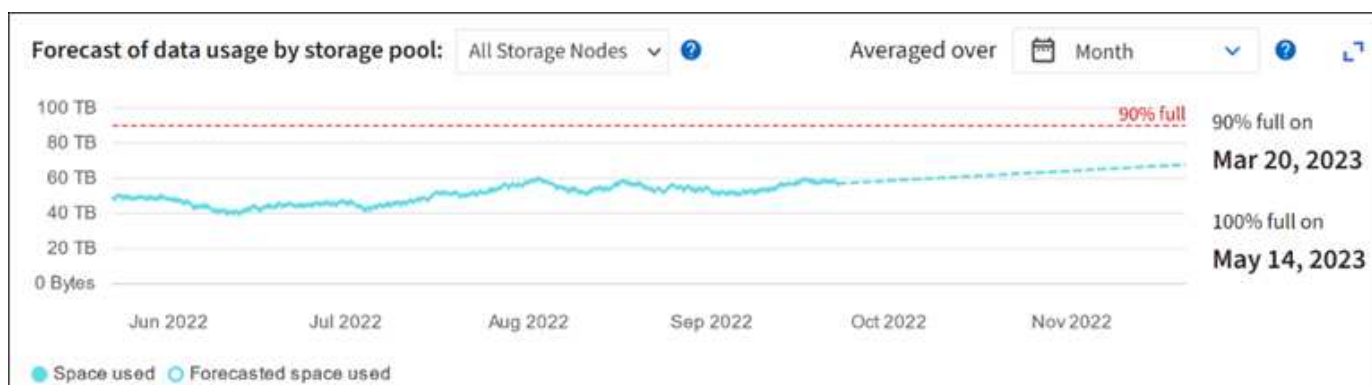
Surveillez les prévisions d'utilisation de l'espace pour les données utilisateur et les métadonnées afin d'estimer quand vous en aurez besoin ["développez une grille"](#).

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 motifs saisonniers, sélectionnez une plage plus longue.

Si vous disposez d'une nouvelle installation StorageGRID, autorisez l'accumulation de données et de métadonnées avant d'évaluer les prévisions d'utilisation de l'espace.

Étapes

1. Sur le tableau de bord, sélectionnez **stockage**.
2. Affichez les cartes du tableau de bord, la prévision de l'utilisation des données par pool de stockage et la prévision de l'utilisation des métadonnées par site.
3. Utilisez ces valeurs pour déterminer quand ajouter de nouveaux nœuds de stockage pour le stockage des données et des métadonnées.



Surveillez la gestion du cycle de vie des informations dans StorageGRID

Le système de gestion du cycle de vie des informations (ILM) assure la gestion des données de tous les objets stockés sur la grille. Vous devez contrôler les opérations ILM pour déterminer si la grille peut gérer la charge actuelle ou si des ressources supplémentaires sont nécessaires.

Description de la tâche

Le système StorageGRID gère les objets en appliquant les règles ILM actives. 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 la gestion des règles ILM. Le système peut ainsi mettre en file d'attente des objets dont les instructions de placement des règles ILM ne peuvent pas être exécutées en temps quasi réel. Vous devez vérifier si StorageGRID est au fait des actions des clients.

Utilisez l'onglet Tableau de bord de Grid Manager

Étapes

Pour contrôler les opérations ILM, utilisez l'onglet ILM du tableau de bord Grid Manager :

1. Connectez-vous au Grid Manager.
2. Dans le tableau de bord, sélectionnez l'onglet ILM et notez les valeurs sur la carte ILM queue (Objects) et la carte des taux d'évaluation ILM.

Des pics temporaires sont attendus dans la carte de la file d'attente ILM (objets) du tableau de bord. Toutefois, si la file d'attente continue d'augmenter ou de ne jamais diminuer, le grid a besoin de davantage de ressources pour fonctionner efficacement : plus de nœuds de stockage ou, si la règle ILM place des objets sur des sites distants, plus de bande passante réseau.

Utiliser la page Nœuds

Étapes

De plus, examinez les files d'attente ILM à l'aide de la page **Nœuds** :



Les graphiques de la page **Nœuds** seront remplacés par les cartes de tableau de bord correspondantes dans une future version de StorageGRID .

1. Sélectionnez **Nœuds**.
2. Sélectionnez **grid name > ILM**.
3. Positionnez le curseur de votre souris sur le graphique de la file d'attente ILM pour voir la valeur des attributs suivants à un moment donné :
 - **Objets mis en file d'attente (à partir des opérations client)** : nombre total d'objets en attente d'évaluation ILM en raison des opérations client (par exemple, ingestion).
 - **Objets mis en file d'attente (de toutes les opérations)** : nombre total d'objets en attente d'évaluation ILM.
 - **Taux d'acquisition (objets/s)** : vitesse à laquelle les objets de la grille sont analysés et mis en file d'attente pour ILM.

- **Taux d'évaluation (objets/s)** : taux actuel auquel les objets sont évalués par rapport à la politique ILM de la grille.



La section de file d'attente ILM est incluse pour la grille uniquement. Ces informations ne s'affichent pas dans l'onglet ILM d'un site ou d'un nœud de stockage.

4. Dans la section ILM Queue, observez les attributs suivants.

- **Période d'analyse - estimation** : temps estimé pour effectuer une analyse ILM complète de tous les objets.



Une analyse complète ne garantit pas l'application du ILM à tous les objets.

- **Tentatives de réparation** : nombre total d'opérations de réparation d'objets pour les données répliquées qui ont été tentées. Ce nombre est incrémenté chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Les réparations ILM à haut risque sont hiérarchisées si le grid est occupé.

La 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.

5. Vous pouvez également soumettre une requête Prometheus pour `storagegrid_ilm_scan_period_estimated_minutes` et `storagegrid_ilm_repairs_attempted`.

Surveillez les ressources réseau et système dans StorageGRID

L'intégrité et la bande passante du réseau entre les nœuds et les sites, ainsi que l'utilisation des ressources par les nœuds de grid individuels, sont essentielles à l'efficacité des opérations.

Contrôle des connexions réseau et des performances

La connectivité réseau et la bande passante sont d'autant plus importantes si votre stratégie de gestion du cycle de vie des informations (ILM) copie les objets répliqués entre des sites ou stocke des objets avec code d'effacement au moyen d'un système qui assure la protection contre la perte de site. Si le réseau entre les sites n'est pas disponible, que la latence du réseau est trop élevée ou que la bande passante du réseau est insuffisante, certaines règles ILM risquent de ne pas pouvoir placer les objets là où prévu. Cela peut entraîner des échecs d'ingestion (lorsque l'option d'ingestion stricte est sélectionnée pour les règles ILM) ou de mauvaises performances d'ingestion et de journalisation des règles ILM.

Utilisez le gestionnaire de grille pour surveiller la connectivité et les performances du réseau, afin de résoudre rapidement tout problème.

Vous pouvez également "[création de stratégies de classification du trafic réseau](#)" surveiller le trafic lié à des locataires, des compartiments, des sous-réseaux ou des terminaux d'équilibrage de la charge. Vous pouvez définir des règles de limitation du trafic selon vos besoins.

Étapes

1. Sélectionnez **Nœuds**.

La page nœuds s'affiche. Chaque nœud de la grille est répertorié au format de tableau.

DASHBOARD
ALERTS
Current
Resolved
Silences
Rules
Email setup
NODES
TENANTS
ILM
CONFIGURATION
MAINTENANCE
SUPPORT

Nodes

View the list and status of sites and grid nodes.

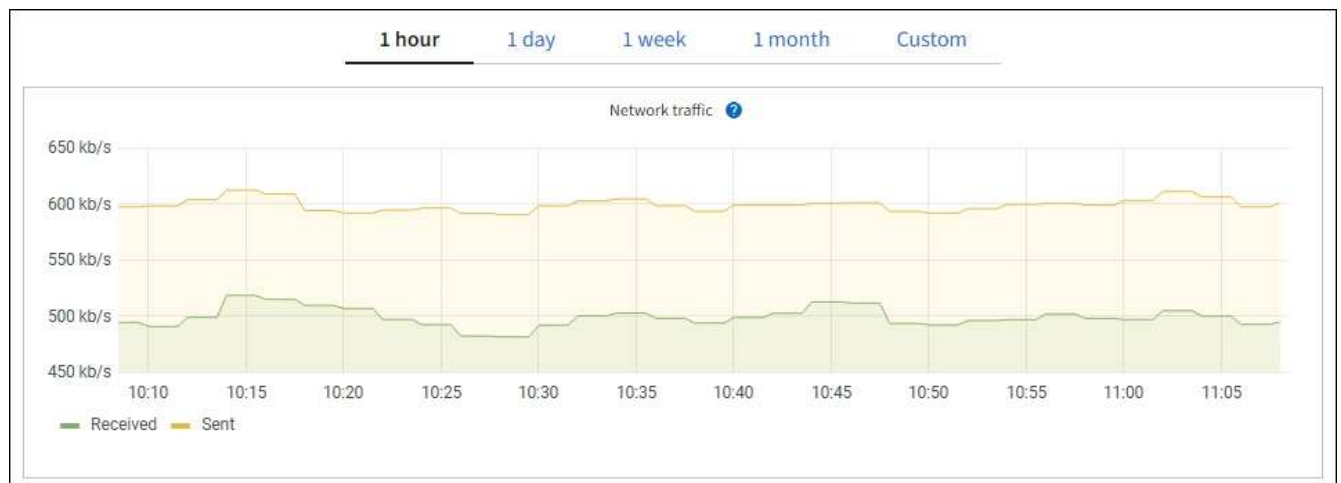
Search... Q

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%

- Sélectionnez le nom de la grille, un site de centre de données spécifique ou un nœud de grille, puis sélectionnez l'onglet **réseau**.

Le graphique trafic réseau fournit un récapitulatif du trafic réseau global pour la grille dans son ensemble, le site du centre de données ou le nœud.



- 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

- Pour les nœuds de grille, faites défiler vers le bas pour consulter la section **communication réseau** de la page.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.

3. Utilisez les indicateurs associés à vos stratégies de classification de trafic pour surveiller le trafic réseau.
 - a. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

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 présentant les indicateurs de réseau associés à une politique, sélectionnez le bouton radio situé à gauche de la politique, puis sélectionnez **Metrics**.
 - b. Consultez les graphiques pour comprendre le trafic réseau associé à la stratégie.

Si une politique de classification du trafic est conçue pour limiter le trafic réseau, analysez la fréquence à laquelle le trafic est limité et déterminez si la politique continue de répondre à vos besoins. De temps en temps [ajustez chaque stratégie de classification du trafic au besoin](#), .

Informations associées

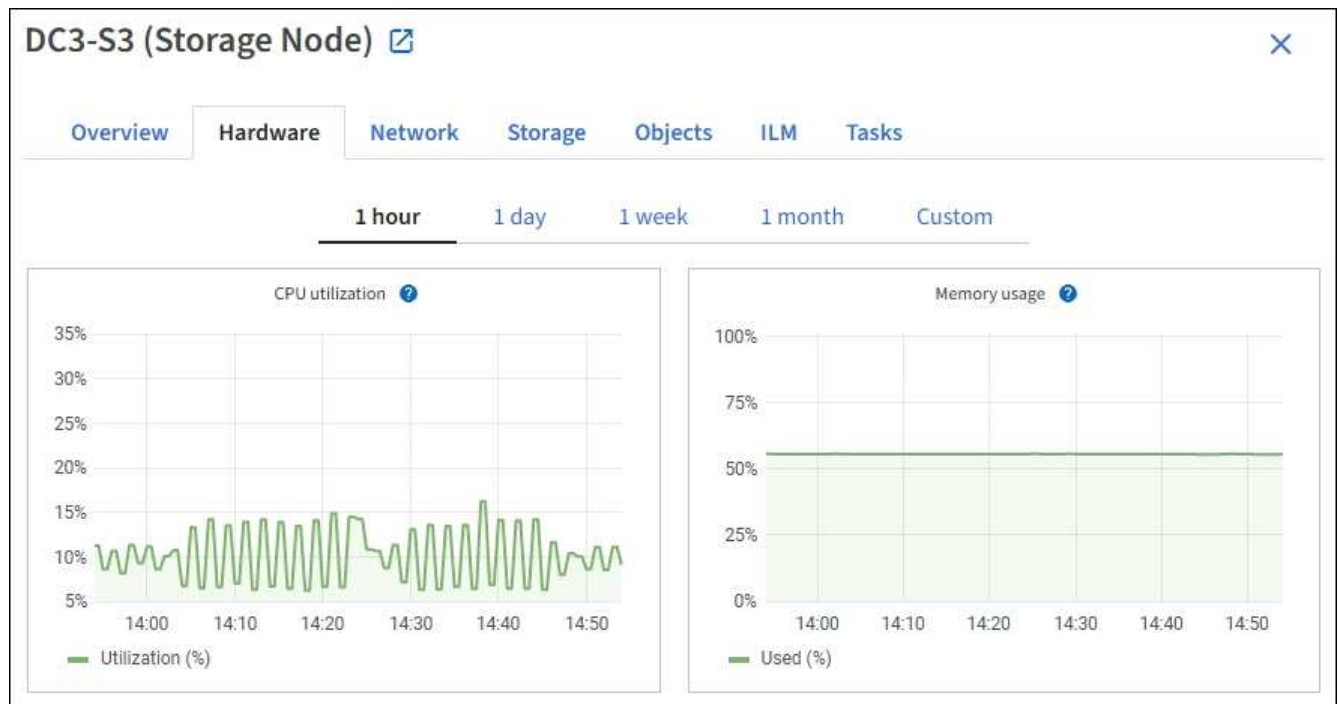
- ["Afficher l'onglet réseau"](#)
- ["Surveiller les États de connexion du nœud"](#)

Contrôle des ressources au niveau des nœuds

Surveiller les nœuds de grid individuels pour vérifier leurs niveaux d'utilisation des ressources. Si les nœuds sont constamment surchargés, un nombre plus élevé de nœuds peut être requis pour une efficacité optimale des opérations.

Étapes

1. Depuis la page **Nœuds**, sélectionnez le nœud.
2. Sélectionnez l'onglet **matériel** pour afficher les graphiques de l'utilisation de l'UC et de la mémoire.



3. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.
4. Si le nœud est hébergé sur une appliance de stockage ou sur une appliance de services, faites défiler la page vers le bas pour afficher les tableaux des composants. L'état de tous les composants doit être « nominal ». Rechercher les composants ayant un autre état.

Informations associées

- ["Afficher des informations sur les nœuds de stockage de l'appliance"](#)
- ["Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle"](#)

Surveillez l'activité des locataires dans StorageGRID

Toutes les activités du client S3 sont associées aux comptes de locataires StorageGRID. Vous pouvez utiliser Grid Manager pour surveiller l'utilisation du stockage ou le trafic réseau de tous les locataires ou d'un locataire spécifique. Vous pouvez utiliser le journal des audits ou les tableaux de bord Grafana pour collecter des informations plus détaillées sur l'utilisation de StorageGRID par les locataires.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine ou de comptes de locataires"](#).

Afficher tous les locataires

La page tenants affiche les informations de base pour tous les comptes de locataires actuels.

Étapes

1. Sélectionnez **Locataires**.

2. Vérifiez les informations affichées sur les pages tenant.

L'espace logique utilisé, l'utilisation des quotas, le quota et le nombre d'objets sont indiqués pour chaque locataire. Si aucun quota n'est défini pour un locataire, les champs utilisation du quota et quota contiennent un tiret (—).



La taille logique de tous les objets appartenant à ce locataire inclut les téléchargements multipartites incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. 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.

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 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 Sign in → dans la colonne **Sign in/Copy URL**.
4. Vous pouvez également copier l'URL de la page de Sign in d'un locataire en sélectionnant le lien de copie d'URL 📄 dans la colonne **Sign in/Copier l'URL**.
5. Si vous le souhaitez, sélectionnez **Exporter au format CSV** pour afficher et exporter un .csv fichier contenant les valeurs d'utilisation de tous les locataires.

Vous êtes invité à ouvrir ou enregistrer le .csv fichier.

Le contenu du .csv 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	1100000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	47500000000	95	1400000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

Vous pouvez ouvrir .csv le fichier dans une feuille de calcul ou l'utiliser dans l'automatisation.

6. Si aucun objet n'est répertorié, sélectionnez **actions** > **Supprimer** pour supprimer un ou plusieurs locataires. Voir "[Supprimer le compte de locataire](#)".

Vous ne pouvez pas supprimer un compte de locataire si le compte inclut des compartiments ou des conteneurs.

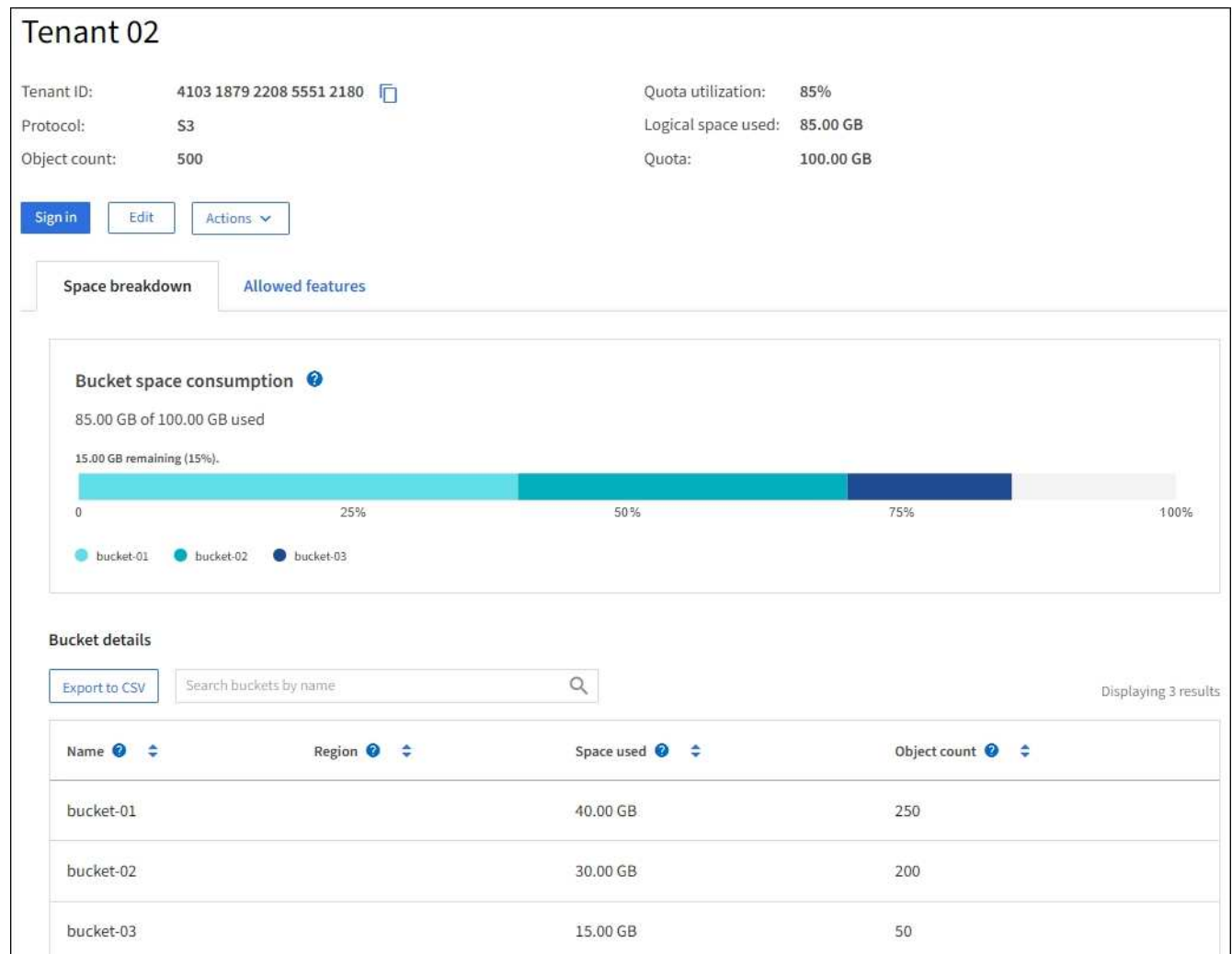
Afficher un locataire spécifique

Vous pouvez afficher les détails d'un locataire spécifique.

Étapes

1. Sélectionnez le nom du locataire dans la page locataires.

La page des détails du locataire s'affiche.



2. Consultez la présentation du locataire en haut de la page.

Cette section de la page de détails fournit des informations récapitulatives pour le locataire, notamment le nombre d'objets du locataire, l'utilisation du quota, l'espace logique utilisé et le paramètre de quota.



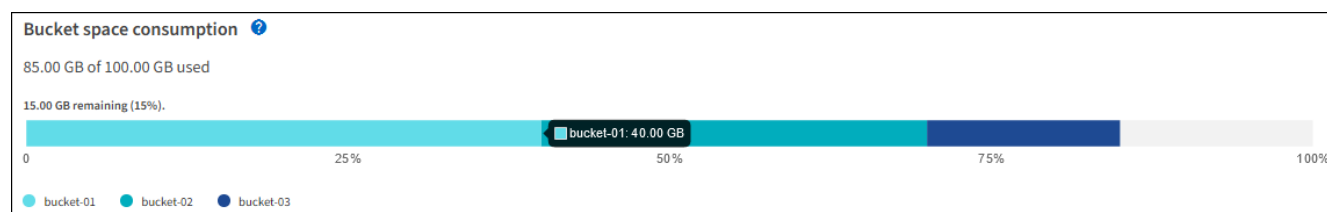
La taille logique de tous les objets appartenant à ce locataire inclut les téléchargements multipartites incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.

3. Dans l'onglet **Space Dclaquage**, consultez le graphique **Space Consumption**.

Ce tableau présente la consommation totale d'espace pour tous les compartiments S3 du locataire.

Si un quota a été défini pour ce tenant, le montant du quota utilisé et restant est affiché dans le texte (par exemple, 85.00 GB of 100 GB used). Si aucun quota n'a été défini, le locataire a un quota illimité et le texte ne contient qu'une quantité d'espace utilisée (par exemple, 85.00 GB used). Le graphique à barres indique le pourcentage de quota dans chaque compartiment ou conteneur. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique indique le quota total et le montant de l'excès.

Vous pouvez placer le curseur sur le graphique à barres pour voir le stockage utilisé par chaque compartiment ou conteneur. Vous pouvez placer votre curseur sur le segment de l'espace libre pour voir la quantité de quota de stockage restant.



L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.



L'utilisation du quota d'un locataire indique la quantité totale de données d'objet chargées par ce dernier sur StorageGRID (taille logique). L'utilisation du quota ne représente pas l'espace utilisé pour stocker des copies de ces objets et de leurs métadonnées (taille physique).



Vous pouvez activer la règle d'alerte **tenant quota usage high** pour déterminer si les locataires utilisent leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour obtenir des instructions, reportez-vous à la section "[Modifiez les règles d'alerte](#)".

4. Dans l'onglet **Space Dclaquage**, passez en revue les détails **Bucket Details**.

Ce tableau répertorie les compartiments S3 pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le compartiment ou le conteneur. Cette valeur ne représente pas l'espace de stockage requis pour les copies ILM et les métadonnées d'objet.

5. Vous pouvez également sélectionner **Exporter au format CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de chaque compartiment ou conteneur.

Le contenu du fichier d'un locataire S3 .csv se présente comme suit :

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 .csv le fichier dans une feuille de calcul ou l'utiliser dans l'automatisation.

6. Vous pouvez également sélectionner l'onglet **fonctions autorisées** pour afficher la liste des autorisations et fonctionnalités activées pour le tenant. Vérifiez ["Modifiez le compte de tenant"](#) si vous avez besoin de modifier l'un de ces paramètres.
7. Si le locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez éventuellement l'onglet **fédération de grille** pour en savoir plus sur la connexion.

Voir ["Qu'est-ce que la fédération de grille ?"](#) et ["Gérer les locataires autorisés pour la fédération dans le grid"](#).

Affichez le trafic réseau

Si des stratégies de classification du trafic sont en place pour un locataire, examinez le trafic réseau de ce locataire.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Consultez la liste des politiques pour identifier celles qui s'appliquent à un locataire spécifique.
3. Pour afficher les mesures associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie et sélectionnez **métriques**.
4. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Voir ["Gérer les stratégies de classification du trafic"](#) pour plus d'informations.

Utilisez le journal d'audit

Vous pouvez également utiliser le journal des audits pour une surveillance plus granulaire des activités d'un locataire.

Par exemple, vous pouvez surveiller les types d'informations suivants :

- Des opérations client spécifiques, telles QUE METTRE, OBTENIR ou SUPPRIMER
- Tailles d'objet
- Règle ILM appliquée aux objets

- Adresse IP source des requêtes client

Les journaux d'audit sont écrits dans des fichiers texte que vous pouvez analyser à l'aide de l'outil d'analyse des journaux de votre choix. Vous pouvez ainsi mieux comprendre les activités des clients ou implémenter des modèles de facturation et de refacturation sophistiqués.

Voir ["Examiner les journaux d'audit"](#) pour plus d'informations.

Utilisez des metrics Prometheus

Éventuellement, utilisez des metrics Prometheus pour générer des rapports sur l'activité des locataires.

- Dans le gestionnaire de grille, sélectionnez **Support > Outils > Métriques**. Vous pouvez utiliser 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 au support technique. Certaines fonctions et options de menu de ces outils ne sont intentionnellement pas fonctionnelles.

- En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**. Vous pouvez utiliser les mesures de la section Metrics de l'API de gestion du grid pour créer des règles d'alerte et des tableaux de bord personnalisés pour l'activité des locataires.

Voir ["Examinez les metrics de support"](#) pour plus d'informations.

Surveillez les opérations du client S3 dans StorageGRID

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

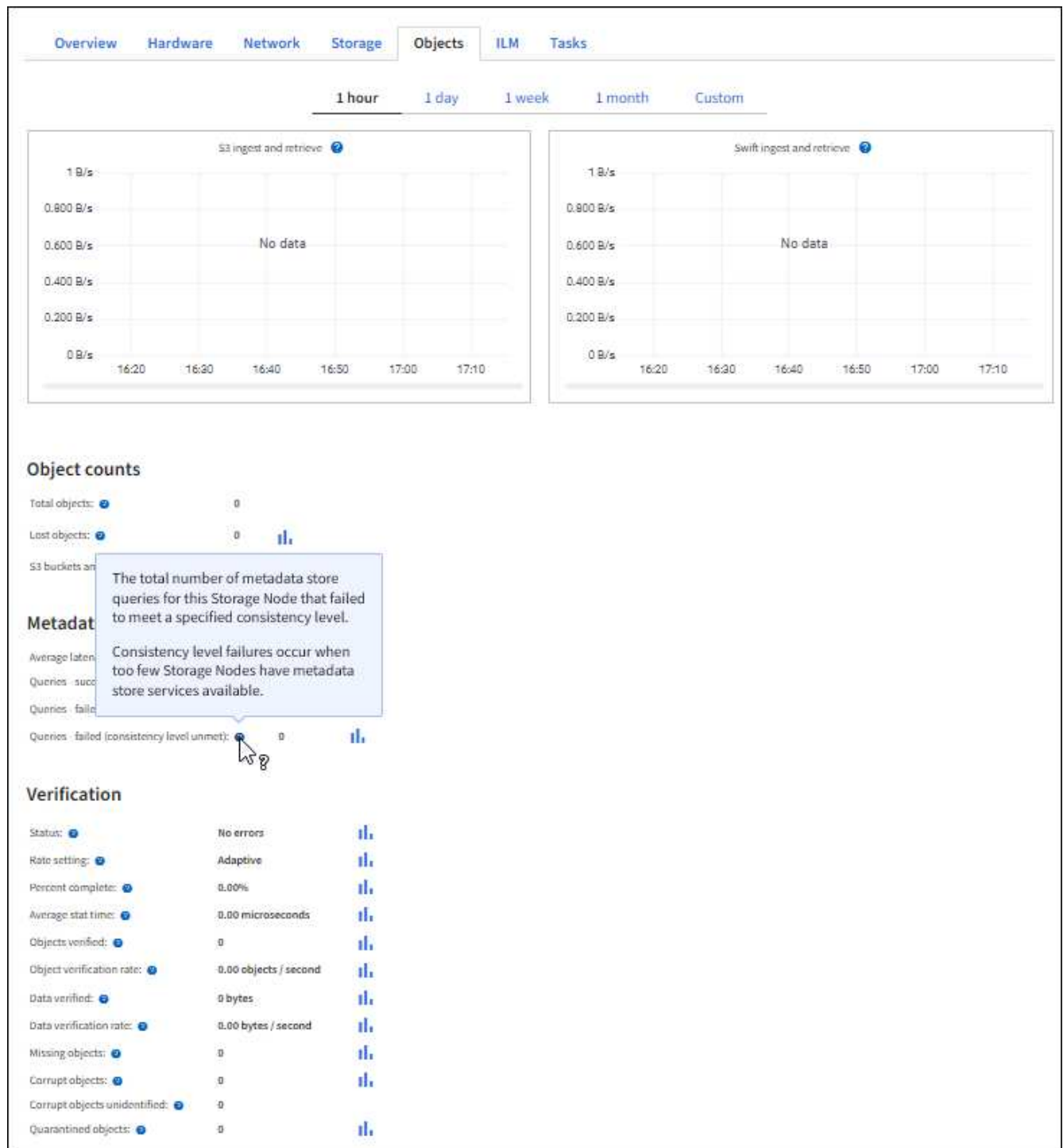
Étapes

1. Dans le tableau de bord, sélectionnez l'onglet **Performance**.
2. Reportez-vous aux graphiques S3, qui résument le nombre d'opérations client effectuées par les nœuds de stockage et le nombre de requêtes d'API reçues par les nœuds de stockage au cours de la période sélectionnée.
3. Sélectionnez **Nœuds** pour accéder à la page Nœuds.
4. Dans la page d'accueil noeuds (niveau grille), sélectionnez l'onglet **objets**.

Le graphique présente les taux d'ingestion et de récupération S3 pour l'ensemble de votre système StorageGRID, en octets par seconde, ainsi que la quantité de données ingérées ou récupérées. Vous pouvez sélectionner un intervalle de temps ou appliquer un intervalle personnalisé.

5. Pour afficher les informations relatives à un nœud de stockage particulier, sélectionnez-le dans la liste de gauche et sélectionnez l'onglet **objets**.

Le graphique présente 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.



Surveillez les opérations d'équilibrage de charge dans StorageGRID

Si vous utilisez un équilibreur de charge pour gérer les connexions client à StorageGRID, vous devez surveiller les opérations d'équilibrage de charge après avoir configuré le système initialement et après avoir effectué des modifications de configuration ou effectué une extension.

Description de la tâche

Vous pouvez utiliser le service Load Balancer sur les nœuds d'administration ou les nœuds de passerelle, ou un équilibreur de charge tiers externe pour distribuer les requêtes client sur plusieurs nœuds de stockage.

Une fois l'équilibrage de la charge configuré, vérifiez que les opérations d'ingestion et de récupération des objets sont réparties de manière homogène entre les nœuds de stockage. La répartition homogène des demandes permet à StorageGRID de rester réactif aux demandes des clients sous charge et de maintenir les performances des clients.

Si vous avez configuré un groupe haute disponibilité de nœuds de passerelle ou de nœuds d'administration en mode de sauvegarde active/active, seul un nœud du groupe distribue activement les requêtes client.

Pour plus d'informations, voir ["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 vous le souhaitez :
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez un nœud de passerelle ou un nœud d'administration.
 - c. Dans l'onglet **Overview**, vérifiez si une interface de nœud fait partie d'un groupe HA et si l'interface de nœud a le rôle Primary.

Les nœuds ayant le rôle de nœud principal et les nœuds qui ne font pas partie d'un groupe haute disponibilité doivent distribuer activement les demandes aux clients.

- d. Pour chaque nœud devant distribuer activement des demandes client, sélectionnez le ["Onglet Load Balancer"](#).
 - e. Consultez le graphique du trafic des demandes d'équilibrage de charge pour la dernière semaine afin de vous assurer que le nœud distribue activement les demandes.

Les nœuds d'un groupe haute disponibilité à sauvegarde active peuvent parfois prendre le rôle de sauvegarde. Pendant ce temps, les nœuds ne distribuent pas les requêtes client.

- f. Consultez le graphique du taux de demande entrant de Load Balancer pour la dernière semaine afin de vérifier le débit d'objet du nœud.
 - g. Répétez cette procédure pour chaque nœud d'administration ou de passerelle du système StorageGRID.
 - h. Vous pouvez également utiliser les stratégies de classification du trafic pour afficher une analyse plus détaillée du trafic desservi par le service Load Balancer.
2. Vérifiez que ces demandes sont réparties de manière homogène vers les nœuds de stockage.
 - a. Sélectionnez **Storage Node > LDR > HTTP**.
 - b. Examiner le nombre de **sessions entrantes actuellement établies**.
 - c. Répétez l'opération pour chaque nœud de stockage de la grille.

Le nombre de sessions doit être approximativement égal sur tous les nœuds de stockage.

Surveiller les connexions de fédération de grille StorageGRID

Vous pouvez surveiller des informations de base sur tous ["connexions de fédération de grille"](#), des informations détaillées sur une connexion spécifique ou des metrics Prometheus sur les opérations de réplication entre les grilles. Vous pouvez surveiller une connexion à partir de l'une ou l'autre des grilles.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#) pour la grille à laquelle vous êtes connecté.

Afficher toutes les connexions

La page Grid federation affiche des informations de base sur toutes les connexions de fédération de grille et sur tous les comptes de locataire autorisés à utiliser les connexions de fédération de grille.

Étapes

1. Sélectionnez **Configuration > Système > Fédération de grille**.

La page grid federation s'affiche.

2. Pour afficher des informations de base sur toutes les connexions de cette grille, sélectionnez l'onglet **connexions**.

À partir de cet onglet, vous pouvez :

- ["Créer une nouvelle connexion"](#).
- Sélectionnez une connexion existante à ["modifier ou tester"](#).

The screenshot shows the 'Grid federation' page. At the top, there's a title 'Grid federation' and a link 'Learn more about grid federation'. Below the title, a paragraph explains that grid federation is used to clone tenant accounts and replicate objects between two StorageGRID systems. The page has two tabs: 'Connections' (active) and 'Permitted tenants'. Under the 'Connections' tab, there are buttons for 'Add connection', 'Upload verification file', and 'Actions', along with a search bar. Below these, a table displays the connection details. The table has three columns: 'Connection name', 'Remote hostname', and 'Connection status'. There is one row showing 'Grid 1 - Grid 2' with hostname '10.96.130.76' and status 'Connected' (indicated by a green checkmark). The text 'Displaying 1 connection' is 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 de locataires de cette grille disposant de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez l'onglet **locataires autorisés**.

À partir de cet onglet, vous pouvez :

- ["Afficher la page de détails pour chaque locataire autorisé"](#).
- Afficher la page de détails de chaque connexion. Voir [Afficher une connexion spécifique](#).
- Sélectionnez un locataire autorisé et ["supprimez l'autorisation"](#).
- Vérifiez la présence d'erreurs de réplication inter-grille et effacez la dernière erreur, le cas échéant. Voir ["Dépanner les erreurs de fédération de grille"](#).

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

permet d'afficher une connexion spécifique

Vous pouvez afficher les détails d'une connexion de fédération de grille spécifique.

Étapes

1. Sélectionnez l'un des onglets de la page fédération de grille, puis sélectionnez le nom de la connexion dans le tableau.

Dans la page de détails de la connexion, vous pouvez :

- Consultez les informations d'état de base sur la connexion, y compris les noms d'hôtes locaux et distants, le port et l'état de la connexion.
- Sélectionnez une connexion à "[modifier, tester ou supprimer](#)".

2. Lors de l'affichage d'une connexion spécifique, sélectionnez l'onglet **locataires autorisés** pour afficher des détails sur les locataires autorisés pour la connexion.

À partir de cet onglet, vous pouvez :

- "[Afficher la page de détails pour chaque locataire autorisé](#)".
- "[Supprimer l'autorisation d'un locataire](#)" pour utiliser la connexion.
- Recherchez les erreurs de réplication inter-grille et effacez la dernière erreur. Voir "[Dépanner les erreurs de fédération de grille](#)".

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	Check for errors

3. Lors de l’affichage d’une connexion spécifique, sélectionnez l’onglet **certificats** pour afficher les certificats de serveur et de client générés par le système pour cette connexion.

À partir de cet onglet, vous pouvez :

- ["Faire pivoter les certificats de connexion"](#).
- Sélectionnez **Server** ou **client** pour afficher ou télécharger le certificat associé ou copier le certificat PEM.

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

EditDownload fileTest connectionRemove

Permitted tenants

Certificates

Rotate certificates

ServerClient

Download certificateCopy 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-----

MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE

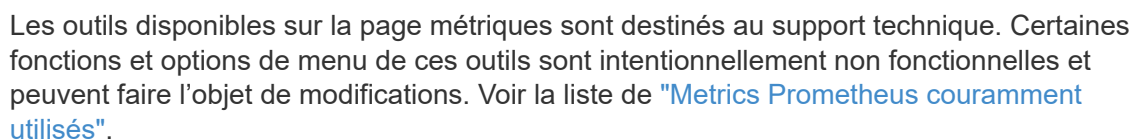
BhMCVVMxExZARBgNVBAGMCKNhbg1mb3JuaWExEjAQBGNVBAcMCVN1bm55dmFsZTEU

NETAPPSUNNYVAZBGNVBAcMCV1bm55dmFsZTEU

-----END CERTIFICATE-----

Vous pouvez utiliser le tableau de bord de réplication Cross-Grid de Grafana pour afficher les metrics Prometheus sur les opérations de réplication cross-grid sur votre grille.

1. Depuis le gestionnaire de grille, sélectionnez **Support > Outils > Métriques**.



- Pour des instructions détaillées, voir ["Examinez les metrics de support"](#).

3. Pour réessayer la réplication d'objets qui n'ont pas pu être répliqués, reportez-vous à la section "[Identifier et réessayer les opérations de réplication ayant échoué](#)".

Gérer les alertes

Gérer les alertes dans StorageGRID

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

Les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions des règles d'alerte sont définies comme vrai. Lorsqu'une alerte est déclenchée, les actions suivantes se produisent :

- Une icône de gravité d'alerte s'affiche sur le tableau de bord dans le Gestionnaire de grille et le nombre d'alertes actuelles est incrémenté.
- L'alerte s'affiche sur la page de résumé **Nœuds** et sur l'onglet **Nœuds > node > Aperçu**.
- Une notification par e-mail est envoyée, en supposant que vous avez configuré un serveur SMTP et fourni des adresses e-mail aux destinataires.
- Une notification SNMP (simple Network Management Protocol) est envoyée, en supposant que vous avez configuré l'agent SNMP StorageGRID.

Vous pouvez créer des alertes personnalisées, modifier ou désactiver des alertes et gérer les notifications d'alerte.

Pour en savoir plus :

- Revoir les vidéos :

[Aperçu des alertes](#)

[Alertes personnalisées](#)

- Reportez-vous à la "[Référence des alertes](#)".

Afficher les règles d'alerte StorageGRID

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 en l'état ou en modifier, ou vous pouvez créer des règles d'alerte personnalisées.

Vous pouvez afficher la liste de toutes les règles d'alerte par défaut et personnalisées pour savoir quelles conditions déclenchent chaque alerte et pour déterminer si les alertes sont désactivées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".
- En option, vous avez regardé la 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. Vérifiez les informations du tableau des règles d'alerte :

En-tête de colonne	Description
Nom	Nom et description uniques de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.

En-tête de colonne	Description
Conditions	Expressions Prometheus qui déterminent le moment où cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de sévérité suivants, mais une condition pour chaque gravité n'est pas requise. • Critique  : Une condition anormale a interrompu le fonctionnement normal d'un nœud ou service StorageGRID. Vous devez résoudre immédiatement le problème sous-jacent. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu. • Majeur  : Une anomalie affecte les opérations en cours ou approche le seuil d'alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tout problème sous-jacent afin de garantir que l'anomalie ne perturbe pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • Mineur  : Le système fonctionne normalement, mais une anomalie existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne se résolvent pas d'elles-mêmes afin de vous assurer qu'elles ne provoquent pas un problème plus grave.
Type	Type de règle d'alerte : • Default : règle d'alerte fournie avec le système. Vous pouvez désactiver une règle d'alerte par défaut ou modifier les conditions et la durée d'une règle d'alerte par défaut. Vous ne pouvez pas supprimer une règle d'alerte par défaut. • Par défaut* : règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée par défaut. • Custom : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.
État	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées et aucune alerte n'est déclenchée.

Créez des règles d'alerte personnalisées dans StorageGRID

Vous pouvez créer des règles d'alerte personnalisées afin de définir vos propres conditions pour déclencher des alertes.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).
- Vous connaissez le ["Metrics Prometheus couramment utilisés"](#).

- Vous comprenez le "[Syntaxe des requêtes Prometheus](#)".
- En option, vous avez regardé la vidéo :

Alertes personnalisées

Description de la tâche

StorageGRID ne valide pas les alertes personnalisées. Si vous décidez de créer des règles d'alerte personnalisées, suivez les consignes générales suivantes :

- Consultez les conditions des règles d'alerte par défaut et utilisez-les comme exemples pour vos règles d'alerte personnalisées.
- Si vous définissez plusieurs conditions pour une règle d'alerte, utilisez la même expression pour toutes les conditions. Modifiez ensuite la valeur seuil pour chaque condition.
- Vérifier soigneusement chaque condition pour détecter les fautes de frappe et les erreurs logiques.
- Utilisez uniquement les metrics répertoriées dans l'API Grid Management.
- Lors du test d'une expression à l'aide de l'API de gestion de grille, sachez qu'une réponse « réussie » peut être un corps de réponse vide (aucune alerte déclenchée). Pour vérifier si l'alerte est déclenchée, vous pouvez définir temporairement une valeur de seuil sur laquelle vous vous attendez à ce que la valeur soit vraie actuellement.

Par exemple, pour tester l'expression `node_memory_MemTotal_bytes < 24000000000`, exécutez d'abord `node_memory_MemTotal_bytes >= 0` et assurez-vous d'obtenir les résultats attendus (tous les nœuds renvoient une valeur). Ensuite, remplacez l'opérateur et le seuil par les valeurs prévues et recommencez. Aucun résultat n'indique qu'il n'y a pas d'alerte en cours pour cette expression.

- Ne supposez pas qu'une alerte personnalisée fonctionne, sauf si vous avez validé que l'alerte est déclenchée quand vous le souhaitez.

Étapes

1. Sélectionnez **Alertes > Règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez **Créer règle personnalisée**.

La boîte de dialogue Créer une règle personnalisée s'affiche.

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

5

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 s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.

Champ	Description
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

5. Dans la section Conditions, entrez une expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.

Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

```
node_memory_MemTotal_bytes < 24000000000
```

Pour consulter les indicateurs disponibles et tester les expressions Prometheus, sélectionnez l'icône d'aide  et suivez le lien vers la section Metrics de l'API de gestion de la grille.

6. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez une unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

La valeur par défaut est 5 minutes.

7. Sélectionnez **Enregistrer**.

La boîte de dialogue se ferme et la nouvelle règle d'alerte personnalisée apparaît dans le tableau règles d'alerte.

Modifier les règles d'alerte dans StorageGRID

Vous pouvez modifier une règle d'alerte pour modifier les conditions de déclenchement, pour une règle d'alerte personnalisée, vous pouvez également mettre à jour le nom de la règle, sa description et les actions recommandées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

- Vous avez le "[Gérer les alertes ou l'autorisation d'accès racine](#)".

Description de la tâche

Lorsque vous modifiez une règle d'alerte par défaut, vous pouvez modifier les conditions pour les alertes mineures, majeures et critiques, ainsi que la durée. Lorsque vous modifiez une règle d'alerte personnalisée, vous pouvez également modifier le nom, la description et les actions recommandées de la règle.



Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne détectiez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

Étapes

1. Sélectionnez **Alertes > Règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio correspondant à la règle d'alerte que vous souhaitez modifier.
3. Sélectionnez **Modifier la règle**.

La boîte de dialogue Modifier la règle s'affiche. Cet exemple montre une règle d'alerte par défaut, les champs Nom unique, Description et actions recommandées sont désactivés et ne peuvent pas être modifiés.

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 que l'alerte n'apparaisse plus comme une alerte active.



En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes si nécessaire.



Vous ne pouvez pas modifier ces informations pour les règles d'alerte par défaut.

Champ	Description
Nom unique	Un nom unique pour cette règle. Le nom de la règle d'alerte s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

6. Dans la section Conditions, entrez ou mettez à jour l'expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.



Si vous souhaitez restaurer une condition pour une règle d'alerte par défaut modifiée à sa valeur d'origine, sélectionnez les trois points à droite de la condition modifiée.

Conditions ?

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



Si vous mettez à jour les conditions d'une alerte en cours, vos modifications risquent de ne pas être appliquées tant que la condition précédente n'est pas résolue. La prochaine fois que l'une des conditions de la règle est remplie, l'alerte reflète les valeurs mises à jour.

Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez l'unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette

valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

La valeur par défaut est 5 minutes.

8. Sélectionnez **Enregistrer**.

Si vous avez modifié une règle d'alerte par défaut, **default*** apparaît dans la colonne Type. Si vous avez désactivé une règle d'alerte par défaut ou personnalisée, **Disabled** apparaît dans la colonne **Status**.

Désactiver les règles d'alerte dans StorageGRID

Vous pouvez modifier l'état activé/désactivé pour une règle d'alerte par défaut ou personnalisée.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

Description de la tâche

Lorsqu'une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

Étapes

1. Sélectionnez **Alertes > Règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio de la règle d'alerte que vous souhaitez désactiver ou activer.

3. Sélectionnez **Modifier la règle**.

La boîte de dialogue Modifier la règle s'affiche.

4. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



Si vous désactivez la règle d'alerte pour une alerte en cours, vous devez attendre quelques minutes que l'alerte ne s'affiche plus comme alerte active.

5. Sélectionnez **Enregistrer**.

Disabled apparaît dans la colonne **Status**.

Supprimez les règles d'alerte personnalisées dans StorageGRID

Vous pouvez supprimer une règle d'alerte personnalisée si vous ne souhaitez plus

l'utiliser.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Alertes > Règles**.

La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio de la règle d'alerte personnalisée que vous souhaitez supprimer.

Vous ne pouvez pas supprimer une règle d'alerte par défaut.

3. Sélectionnez **Supprimer la règle personnalisée**.

Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **OK** pour supprimer la règle d'alerte.

Toutes les instances actives de l'alerte seront résolues dans un délai de 10 minutes.

Gérer les notifications d'alerte

Configurer les notifications SNMP pour les alertes StorageGRID

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, reportez-vous à ["Utiliser la surveillance SNMP"](#) la section.

Après avoir configuré l'agent SNMP StorageGRID, deux types de notifications basées sur les événements peuvent être envoyées :

- Les interruptions sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple. Les traps sont pris en charge dans les trois versions de SNMP.
- Les informations sont similaires aux pièges, mais elles nécessitent une reconnaissance par le système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte. Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Des notifications d'interruption et d'information sont envoyées lorsqu'une alerte par défaut ou personnalisée est déclenchée à n'importe quel niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Voir ["Notifications d'alerte de silence"](#).

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les packages AutoSupport, les traps et les notifications SNMP. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir ["Qu'est-ce qu'un nœud d'administration ?"](#).

Configurer les notifications par e-mail pour les alertes StorageGRID

Si vous souhaitez que des notifications par e-mail soient envoyées lorsque des alertes se produisent, vous devez fournir des informations sur votre serveur SMTP. Vous devez également saisir des adresses e-mail pour les destinataires des notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).
- Vous avez ["configuré un serveur de messagerie"](#).

Description de la tâche

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, les traps et les notifications SNMP. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir ["Qu'est-ce qu'un nœud d'administration ?"](#).

Étapes

1. Sélectionnez **Alertes > Courriel d'alerte**.

La page des alertes par e-mail s'affiche.

2. Cochez la case **Activer les alertes par e-mail** pour indiquer que vous souhaitez que des e-mails de notification soient envoyés lorsque les alertes atteignent les seuils configurés.
3. Dans la section **Recevoir des e-mails par niveau de gravité**, sélectionnez le bouton radio qui indique les types d'alertes pour lesquels vous souhaitez recevoir une notification.
4. Dans la section Expéditeur, spécifiez une adresse électronique valide à utiliser comme adresse d'expéditeur pour les notifications d'alerte.

Par exemple : `storagegrid-alerts@example.com`

- a. Dans la section destinataires, entrez une adresse e-mail pour chaque liste d'e-mails ou personne devant recevoir un e-mail lorsqu'une alerte se produit.

Sélectionnez **Ajouter un destinataire** pour ajouter des destinataires.

5. Sélectionnez **Enregistrer**.

Informations incluses dans les notifications par e-mail d'alerte

Après avoir configuré le serveur de messagerie et activé l'envoi d'e-mails pour les alertes, des notifications par e-mail sont envoyées aux destinataires désignés lorsqu'une alerte est déclenchée, sauf si la règle d'alerte est supprimée par un silence. Reportez-vous à ["Notifications d'alerte de silence"](#).

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

Légende	Description
1	Nom de l'alerte, suivi du nombre d'instances actives de cette alerte.
2	Description de l'alerte.
3	Actions recommandées pour l'alerte.
4	Détails sur chaque instance active de l'alerte, y compris le nœud et le site affectés, la gravité de l'alerte, l'heure UTC au moment où la règle d'alerte a été déclenchée, ainsi que le nom du travail et du service affectés.
5	Nom d'hôte du nœud d'administration qui a envoyé la notification.

Mode de regroupement des alertes

Pour empêcher l'envoi d'un nombre excessif de notifications par e-mail lorsque des alertes sont déclenchées, StorageGRID tente de regrouper plusieurs alertes dans la même notification.

Reportez-vous au tableau suivant pour obtenir des exemples de la manière dont StorageGRID regroupe plusieurs alertes dans les notifications par e-mail.

Comportement	Exemple
Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes avec des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.	• L'alerte A est déclenchée en même temps sur deux nœuds. Une seule notification est envoyée. • L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée simultanément sur le nœud 2. Deux notifications sont envoyées : une pour chaque alerte.
Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un degré de sévérité, une notification est envoyée uniquement pour l'alerte la plus grave.	• L'alerte A est déclenchée et le seuil d'alerte secondaire, majeur et critique est atteint. Une notification est envoyée pour l'alerte critique.
La première fois qu'une alerte est déclenchée, StorageGRID attend 2 minutes avant d'envoyer une notification. Si d'autres alertes du même nom sont déclenchées pendant ce temps, StorageGRID regroupe toutes les alertes de la notification initiale.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Aucune notification n'a été envoyée. 2. L'alerte A est déclenchée sur le nœud 2 à 08:01. Aucune notification n'a été envoyée. 3. À 08 h 02, une notification est envoyée pour signaler les deux instances de l'alerte.
Si une autre alerte du même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes en cours qui n'ont pas été désactivées), même si elles ont été signalées précédemment.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Une notification est envoyée à 08:02. 2. L'alerte A est déclenchée sur le nœud 2 à 08:05. Une seconde notification est envoyée à 08:15 (10 minutes plus tard). Les deux nœuds sont signalés.
Si plusieurs alertes en cours portent le même nom et que l'une de ces alertes est résolue, une nouvelle notification n'est pas envoyée si l'alerte se reproduit sur le nœud pour lequel l'alerte a été résolue.	1. L'alerte A est déclenchée pour le nœud 1. Une notification est envoyée. 2. L'alerte A est déclenchée pour le nœud 2. Une seconde notification est envoyée. 3. L'alerte A est résolue pour le nœud 2, mais elle reste active pour le nœud 1. 4. L'alerte A est à nouveau déclenchée pour le nœud 2. Aucune nouvelle notification n'est envoyée, car l'alerte est toujours active pour le nœud 1.
StorageGRID continue à envoyer des notifications par e-mail tous les 7 jours jusqu'à ce que toutes les instances de l'alerte soient résolues ou que la règle d'alerte soit désactivée.	1. L'alerte A est déclenchée pour le nœud 1 le 8 mars. Une notification est envoyée. 2. L'alerte A n'est pas résolue ou arrêtée. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.

Dépanner les notifications d'alerte par e-mail

Suivez ces étapes pour examiner et résoudre le problème si l'alerte d'échec de notification par e-mail est déclenchée et que vous ne recevez pas :

- Tester les notifications du serveur de messagerie
- Courriels d'alerte StorageGRID
- Courriels de vérification multi-administrateur (MAV)

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous disposez de la ["Autorisation d'accès racine"](#). Si vous disposez de l'autorisation Gérer les alertes, vous pouvez consulter, mais pas modifier, la configuration du serveur de messagerie.

Étapes

1. Vérifiez les paramètres de vos alertes par e-mail.
 - a. Vérifiez que vous avez spécifié des adresses e-mail valides pour les destinataires.
 - b. Sélectionnez **Configuration** > **Serveur de messagerie** et vérifiez que les paramètres du serveur de messagerie (SMTP) sont corrects.
2. Vérifiez votre filtre de spam et assurez-vous que l'e-mail n'a pas été envoyé à un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails de l'adresse de l'expéditeur ne sont pas bloqués.
4. Vérifiez les éléments suivants relatifs au transfert de courriels :
 - a. Surveillance des journaux du serveur de messagerie : consultez les journaux du serveur de messagerie utilisé par StorageGRID (**Configuration** > **Serveur de messagerie**). Recherchez les erreurs de relais, d'authentification et autres défaillances correspondant à l'heure à laquelle StorageGRID a tenté d'envoyer un e-mail.
 - b. Messages de non-distribution (retours d'e-mail) : Si les e-mails ne sont pas reçus et que StorageGRID ne signale aucune erreur, il peut s'agir d'un retour d'e-mail. Configurer l'adresse d'expéditeur pour utiliser une adresse e-mail valide rendra ces messages de retour d'e-mail visibles pour vous.
5. Collectez les fichiers journaux du nœud d'administration qui envoie les e-mails. Examinez les fichiers `/var/local/log/prometheus.log` et `/var/local/log/nms.log` pour détecter les problèmes évidents que vous pourriez corriger. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Le support technique peut utiliser les informations contenues dans les journaux pour vous aider à déterminer ce qui s'est mal passé. Par exemple, le fichier `prometheus.log` peut afficher une erreur lors de la connexion au serveur spécifié.

Consultez ["Collecte de fichiers journaux et de données système"](#).

Désactiver les notifications d'alerte dans StorageGRID

Si vous le souhaitez, vous pouvez configurer des silences pour supprimer temporairement les notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès racine"](#).

Description de la tâche

Vous pouvez désactiver les règles d'alerte sur toute la grille, sur un seul site ou sur un seul nœud et pour une ou plusieurs niveaux de gravité. Chaque silence supprime toutes les notifications d'une règle d'alerte unique ou de toutes les règles d'alerte.

Si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informent.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous neutralisez une alerte, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

Étapes

1. Sélectionnez **Alertes > Silences**.

La page silences s'affiche.

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 une 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 entrez les informations suivantes :

Champ	Description
Règle d'alerte	Le nom de la règle d'alerte que vous souhaitez désactiver. Vous pouvez sélectionner n'importe quelle règle d'alerte par défaut ou personnalisée, même si la règle d'alerte est désactivée. Remarque : sélectionnez toutes les règles si vous voulez désactiver toutes les règles d'alerte en utilisant les critères spécifiés dans cette boîte de dialogue.
Description	Éventuellement, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps vous voulez que ce silence reste en vigueur, en minutes, heures ou jours. Un silence peut être en vigueur de 5 minutes à 1,825 jours (5 ans). Remarque: vous ne devez pas désactiver une règle d'alerte pour une durée prolongée. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique. Cependant, vous devrez peut-être utiliser un silence étendu si une alerte est déclenchée par une configuration intentionnelle spécifique, par exemple pour les alertes liaison appliance Services Down et les alertes liaison appliance Storage Down.

Champ	Description
Gravité	Quelle alerte de gravité ou de gravité doit être neutralisée. Si l'alerte est déclenchée à l'un des niveaux de gravité sélectionnés, aucune notification n'est envoyée.
Nœuds	À quel nœud ou nœud vous souhaitez que ce silence s'applique. Vous pouvez supprimer une règle d'alerte ou toutes les règles de la grille dans son ensemble, un seul site ou un seul nœud. Si vous sélectionnez l'ensemble de la grille, le silence s'applique à tous les sites et à tous les nœuds. Si vous sélectionnez un site, le silence s'applique uniquement aux nœuds de ce site. Note: vous ne pouvez pas sélectionner plus d'un nœud ou plus d'un site pour chaque silence. Vous devez créer des silences supplémentaires si vous souhaitez supprimer la même règle d'alerte sur plusieurs nœuds ou plusieurs sites à la fois.

4. Sélectionnez **Enregistrer**.

5. Si vous souhaitez modifier ou mettre fin à un silence avant son expiration, vous pouvez le modifier ou le supprimer.

Option	Description
Modifier un silence	a. Sélectionnez Alertes > Silences. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez modifier. c. Sélectionnez Modifier. d. Modifiez la description, le temps restant, les niveaux de gravité sélectionnés ou le nœud affecté. e. Sélectionnez Enregistrer.
Supprimer un silence	a. Sélectionnez Alertes > Silences. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez supprimer. c. Sélectionnez Supprimer. d. Sélectionnez OK pour confirmer que vous souhaitez supprimer ce silence. Remarque : les notifications sont maintenant envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est déclenchée, l'envoi de notifications par e-mail ou SNMP peut prendre quelques minutes et la mise à jour de la page alertes.

Informations associées

["Configurez l'agent SNMP"](#)

Alertes dans StorageGRID

Cette référence répertorie les alertes par défaut qui apparaissent dans le Gestionnaire de grille. Les actions recommandées sont dans le message d'alerte que vous recevez.

Si nécessaire, vous pouvez créer des règles d'alerte personnalisées en fonction de votre approche de gestion du système.

Certaines alertes par défaut utilisent ["Metrics Prometheus"](#).

Alertes de l'appliance

Nom de l'alerte	Description
Batterie de l'appareil expirée	La batterie du contrôleur de stockage de l'appareil a expiré.
La batterie de l'appareil est défectueuse	La batterie du contrôleur de stockage de l'appareil est défectueuse.
La capacité de la batterie de l'appareil est insuffisante	La capacité de la batterie du contrôleur de stockage de l'appareil est insuffisante.
La batterie de l'appareil est presque déchargée	La batterie du contrôleur de stockage de l'appliance arrive à expiration.
Batterie de l'appareil retirée	La batterie du contrôleur de stockage de l'appareil est manquante.
Batterie de l'appareil trop chaude	La batterie du contrôleur de stockage de l'appareil est en surchauffe.
Erreur de communication du BMC de l'appliance	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue.
Erreur de périphérique d'amorçage de l'appliance détectée	Un problème a été détecté au niveau du périphérique d'amorçage de l'appareil.
Échec du périphérique de sauvegarde du cache de l'appliance	Échec d'un périphérique de sauvegarde de cache persistant.
Capacité insuffisante du périphérique de sauvegarde en cache de l'appliance	La capacité du périphérique de sauvegarde du cache est insuffisante.
Dispositif de sauvegarde cache de l'appliance protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.
La taille de la mémoire cache de l'appliance ne correspond pas	Le cache des deux contrôleurs de l'appliance est de différentes tailles.

Nom de l'alerte	Description
Défaillance de la pile CMOS de l'appareil	Un problème a été détecté au niveau de la pile CMOS de l'appareil.
La température du châssis du contrôleur de calcul de l'appliance est trop élevée	La température du contrôleur de calcul d'une appliance StorageGRID a dépassé le seuil nominal.
Température trop élevée du processeur du contrôleur de calcul de l'appliance	La température du processeur dans le contrôleur de calcul d'une appliance StorageGRID a dépassé le seuil nominal.
Le contrôleur de calcul de l'appliance doit faire attention	Une défaillance matérielle a été détectée dans le contrôleur de calcul d'une appliance StorageGRID.
L'alimentation A du contrôleur de calcul de l'appliance présente un problème	L'alimentation A du contrôleur de calcul présente un problème.
L'alimentation B du contrôleur de calcul de l'appliance présente un problème	L'alimentation B du contrôleur de calcul présente un problème.
Service de surveillance du matériel de calcul de l'appliance bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.
Disques DAS du dispositif dépassant la limite pour les données écrites par jour	Une quantité excessive de données est écrite sur un disque chaque jour, ce qui pourrait annuler sa garantie.
Panne du lecteur DAS de l'appliance détectée	Un problème a été détecté au niveau d'un disque DAS (Direct-Attached Storage) dans l'appliance.
Le lecteur DAS de l'appareil se trouve dans le mauvais emplacement ou le mauvais nœud	Un lecteur de stockage à connexion directe (DAS) se trouve dans le mauvais emplacement ou le mauvais nœud
Le voyant de localisation du dispositif DAS est allumé	Le voyant de localisation de lecteur d'un ou plusieurs disques DAS (Direct-Attached Storage Node) d'un nœud de stockage d'appliance est allumé.
Reconstruction des disques DAS du dispositif	Un disque DAS (Direct-Attached Storage) est en cours de reconstruction. Ceci est attendu s'il a été récemment remplacé ou supprimé/réinséré.
Panne du ventilateur de l'appareil détectée	Un problème de ventilateur dans l'appareil a été détecté.

Nom de l'alerte	Description
Panne Fibre Channel de l'appliance détectée	Un problème de liaison Fibre Channel a été détecté entre le contrôleur de stockage de l'appliance et le contrôleur de calcul
Défaillance du port HBA Fibre Channel de l'appliance	Un port HBA Fibre Channel est défectueux ou est défectueux.
Flash cache de l'appliance ne sont pas optimaux	Les disques utilisés pour la mise en cache SSD ne sont pas optimaux.
Interconnexion de l'appareil/boîtier de la batterie retiré	Le boîtier d'interconnexion/de batterie est manquant.
Port d'appliance LACP manquant	Aucun port d'une appliance StorageGRID ne participe au lien LACP.
Défaillance de la carte réseau de l'appareil détectée	Un problème de carte d'interface réseau (NIC) a été détecté sur le serveur.
L'alimentation générale de l'appareil est dégradée	La puissance d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.
Mise à jour du logiciel du système d'exploitation SANtricity requise	La version du logiciel SANtricity est inférieure au minimum recommandé pour cette version de StorageGRID.
Défaut SFP détecté sur l'appareil	Une panne SFP a été détectée dans le contrôleur de calcul d'une appliance StorageGRID.
Avertissement critique sur les disques SSD de l'appliance	Un SSD d'appliance signale un avertissement critique.
Défaillance Du contrôleur de stockage De l'appliance	Le contrôleur de stockage A d'une appliance StorageGRID est en panne.
Défaillance du contrôleur B de stockage de l'appliance	Le contrôleur de stockage B d'une appliance StorageGRID est en panne.
Panne de disque du contrôleur de stockage de l'appliance	Un ou plusieurs disques d'une appliance StorageGRID sont défectueux ou non optimaux.
Problème matériel du contrôleur de stockage de l'appliance	Le logiciel SANtricity signale les besoins d'attention d'un composant d'une appliance StorageGRID.
Panne de l'alimentation Du contrôleur de stockage de l'appliance	L'alimentation A d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.

Nom de l'alerte	Description
Panne de l'alimentation B du contrôleur de stockage de l'appliance	L'alimentation B d'un dispositif StorageGRID s'est déviée de la tension de fonctionnement recommandée.
Entretien du moniteur matériel de stockage de l'appliance bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.
Dégradation des tiroirs de stockage de l'appliance	L'état de l'un des composants du tiroir de stockage d'une appliance de stockage est dégradé.
Température de l'appareil dépassée	La température nominale ou maximale du contrôleur de stockage de l'appareil a été dépassée.
Capteur de température de l'appareil retiré	Un capteur de température a été déposé.
Erreur d'amorçage sécurisé UEFI de l'appliance	Un appareil n'a pas été correctement démarré.
Les E/S du disque sont très lentes	Les E/S de disque très lentes peuvent affecter les performances du grid.
Panne du ventilateur du dispositif de stockage détectée	Un problème de ventilateur dans le contrôleur de stockage d'un dispositif a été détecté.
Dégradation de la connectivité du stockage de l'appliance de stockage	Un problème se produit au niveau d'une ou plusieurs connexions entre le contrôleur de calcul et le contrôleur de stockage.
Périphérique de stockage inaccessible	Impossible d'accéder à un périphérique de stockage.

Alertes d'audit et syslog

Nom de l'alerte	Description
Des journaux d'audit sont ajoutés à la file d'attente en mémoire	Le nœud ne peut pas envoyer de journaux au serveur syslog local et la file d'attente in-memory est en cours de remplissage.
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 risquent d'échouer.
Des journaux sont ajoutés à la file d'attente sur disque	Le nœud ne peut pas transférer les journaux vers le serveur syslog externe et la file d'attente sur disque est en cours de chargement.

Alertes de compartiment

Nom de l'alerte	Description
Le paramètre de cohérence du compartiment FabricPool n'est pas pris en charge	Un compartiment FabricPool utilise le niveau de cohérence disponible ou élevé des sites, ce qui n'est pas pris en charge.
Le compartiment FabricPool possède un paramètre de gestion des versions non pris en charge	La gestion des versions ou le verrouillage d'objet S3 d'un compartiment FabricPool est activé, ce qui n'est pas pris en charge.
ListBucket vérification des autorisations pour Get/Head object désactivée	ListBucket la vérification des autorisations pour GetObject/HeadObject sur des clés inexistantes est désactivée.

Alertes Cassandra

Nom de l'alerte	Description
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.
Indicateurs du compacteur automatique Cassandra obsolètes	Les mesures qui décrivent le compacteur automatique Cassandra sont obsolètes.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra rencontrent des problèmes.
Compression Cassandra surchargée	Le processus de compactage Cassandra est surchargé.
Erreur d'écriture surdimensionnée Cassandra	Un processus StorageGRID interne a envoyé à Cassandra une demande d'écriture trop volumineuse.
Les metrics de réparation de Cassandra sont obsolètes	Les mesures qui décrivent les tâches de réparation de Cassandra sont obsolètes.
La progression de la réparation de Cassandra est lente	La progression des réparations des bases de données Cassandra est lente.
Le service de réparation Cassandra n'est pas disponible	Le service de réparation Cassandra n'est pas disponible.
La corruption des tables Cassandra	Cassandra a détecté une corruption de table. Cassandra redémarre automatiquement si elle détecte une corruption de la table.

Alertes de pool de stockage cloud

Nom de l'alerte	Description
Erreur de connectivité de Cloud Storage Pool	Le contrôle de l'état des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs.
IAM Roles Anywhere expiration de la certification d'entité finale	Le certificat d'entité finale IAM Roles Anywhere va expirer.

Alertes de réplication intergrid

Nom de l'alerte	Description
Défaillance permanente de la réplication entre les grilles	Une erreur de réplication inter-grille s'est produite et nécessite une intervention de l'utilisateur pour la résoudre.
Ressources de réplication intergrid indisponibles	Les demandes de réplication multigrille sont en attente car une ressource n'est pas disponible.

Alertes DHCP

Nom de l'alerte	Description
Bail DHCP expiré	Le bail DHCP sur une interface réseau a expiré.
La location DHCP expire bientôt	Le bail DHCP sur une interface réseau expire bientôt.
Serveur DHCP indisponible	Le serveur DHCP n'est pas disponible.

Alertes de débogage et de suivi

Nom de l'alerte	Description
Impact sur les performances de débogage	Lorsque le mode débogage est activé, les performances du système peuvent être affectées négativement.
Configuration de trace activée	Lorsque la configuration de trace est activée, les performances du système peuvent être affectées de façon négative.

Alertes par e-mail et AutoSupport

Nom de l'alerte	Description
Échec de l'envoi du message AutoSupport	L'envoi du message AutoSupport le plus récent a échoué.

Nom de l'alerte	Description
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	Impossible d'envoyer la notification par e-mail pour une alerte.
Le bucket de destination d'archivage des journaux est introuvable	Le bucket de destination d'archivage des journaux est manquant, ce qui empêche l'archivage des journaux dans le bucket de destination.
Erreurs d'information SNMP	Erreurs lors de l'envoi de notifications d'information SNMP à une destination d'interruption.
Accès externe SSH activé	L'accès externe SSH est activé depuis plus de 24 heures.
Connexion SSH ou console détectée	Au cours des 24 dernières heures, un utilisateur s'est connecté à la console Web ou à SSH.

Alertes de code d'effacement (EC)

Nom de l'alerte	Description
Nombre élevé de goroutines du service de chunk	Le service de chunk présente un nombre anormalement élevé de goroutines, ce qui pourrait indiquer un deadlock ou une fuite de ressources.
Défaillance du rééquilibrage EC	La procédure de rééquilibrage EC a échoué ou a été arrêtée.
Échec de réparation EC	Une tâche de réparation pour les données EC a échoué ou a été arrêtée.
Réparation EC bloquée	Un travail de réparation pour les données EC est bloqué.
Erreur de vérification de fragment avec code d'effacement	Les fragments avec code d'effacement ne peuvent plus être vérifiés. Des fragments corrompus peuvent ne pas être réparés.
Groupes à codage d'effacement en état Needs Repair	Un ou plusieurs groupes codés par effacement sont dans l'état « Nécessite une réparation » alors qu'aucune réparation de données codées par effacement n'est en cours.

Expiration des alertes de certificats

Nom de l'alerte	Description
Expiration du certificat de l'autorité de certification du proxy d'administration	Un ou plusieurs certificats du paquet CA du serveur proxy d'administration sont sur le point d'expirer.

Nom de l'alerte	Description
Expiration du certificat client	Un ou plusieurs certificats client sont sur le point d'expirer.
Expiration du certificat de serveur global pour S3	Le certificat de serveur global pour S3 est sur le point d'expirer.
Expiration du certificat de point final de l'équilibreur de charge	Un ou plusieurs certificats de noeud final de l'équilibreur de charge vont expirer.
Expiration du certificat de serveur pour l'interface de gestion	Le certificat de serveur utilisé pour l'interface de gestion est sur le point d'expirer.
Expiration du certificat d'autorité de certification syslog externe	Le certificat d'autorité de certification (CA) utilisé pour signer le certificat de serveur syslog externe est sur le point d'expirer.
Expiration du certificat du client syslog externe	Le certificat client d'un serveur syslog externe est sur le point d'expirer.
Expiration du certificat du serveur syslog externe	Le certificat de serveur présenté par le serveur syslog externe arrive à expiration.

Alertes réseau Grid

Nom de l'alerte	Description
Non-concordance de MTU du réseau de grid	Le paramètre MTU de l'interface réseau Grid (eth0) diffère de manière significative sur tous les nœuds de la grille.

Alertes de fédération du grid

Nom de l'alerte	Description
Expiration du certificat de fédération GRID	Un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.
Échec de la connexion de fédération de grille	La connexion de fédération de grille entre la grille locale et la grille distante ne fonctionne pas.

Alertes d'utilisation élevée ou de latence élevée

Nom de l'alerte	Description
Latence élevée pour les requêtes de métadonnées	La durée moyenne des requêtes de métadonnées Cassandra est trop longue.

Alertes de fédération des identités

Nom de l'alerte	Description
Échec de synchronisation de la fédération d'identités	Impossible de synchroniser des groupes fédérés et des utilisateurs à partir du référentiel d'identité.
Échec de la synchronisation de la fédération des identités pour un locataire	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir du référentiel d'identité configuré par un locataire.

Alertes de gestion du cycle de vie des informations (ILM)

Nom de l'alerte	Description
Placement ILM impossible à atteindre	Une instruction de placement dans une règle ILM ne peut pas être obtenue pour certains objets.
Taux d'analyse ILM faible	La vitesse d'analyse ILM est définie sur moins de 100 objets/seconde.

Alertes du serveur de gestion des clés (KMS)

Nom de l'alerte	Description
Expiration du certificat CA KMS	Le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion des clés (KMS) est sur le point d'expirer.
Expiration du certificat client KMS	Le certificat client d'un serveur de gestion des clés est sur le point d'expirer
Echec du chargement de la configuration DES KMS	La configuration du serveur de gestion des clés existe mais n'a pas pu être chargée.
Erreur de connectivité KMS	Un nœud d'appliance n'a pas pu se connecter au serveur de gestion des clés de son site.
Nom de la clé de cryptage KMS introuvable	Le serveur de gestion des clés configuré ne dispose pas d'une clé de chiffrement correspondant au nom fourni.
Echec de la rotation de la clé de chiffrement KMS	Tous les volumes de l'appliance ont été décryptés avec succès, mais un ou plusieurs volumes n'ont pas pu tourner vers la clé la plus récente.
LES KMS ne sont pas configurés	Aucun serveur de gestion des clés n'existe pour ce site.
La clé KMS n'a pas réussi à décrypter un volume d'appliance	Impossible de décrypter un ou plusieurs volumes sur une appliance dont le chiffrement de nœud est activé avec la clé KMS actuelle.

Nom de l'alerte	Description
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.
Echec de la connectivité du serveur KM	Un nœud d'appliance n'a pas pu se connecter à un ou plusieurs serveurs du cluster de serveurs de gestion des clés pour son site.

Alertes d'équilibrage de la charge

Nom de l'alerte	Description
Des connexions élevées d'équilibreur de charge sans demande	Pourcentage élevé de connexions aux terminaux de l'équilibreur de charge déconnectés sans effectuer de requêtes.

Alertes de décalage d'horloge locale

Nom de l'alerte	Description
Décalage horaire grand horloge locale	Le décalage entre l'horloge locale et l'heure NTP (Network Time Protocol) est trop important.

Alertes de mémoire insuffisante ou d'espace insuffisant

Nom de l'alerte	Description
Capacité du disque du journal d'audit faible	L'espace disponible pour les journaux d'audit est faible. Si cette condition n'est pas résolue, les opérations S3 risquent d'échouer.
Mémoire de nœud faible disponibilité	La quantité de RAM disponible sur un nœud est faible.
Faible espace libre pour le pool de stockage	L'espace disponible pour le stockage des données d'objet dans le nœud de stockage est faible.
Mémoire insuffisante sur les nœuds installés	La quantité de mémoire installée sur un nœud est faible.
Faibles capacités de stockage de métadonnées	L'espace disponible pour le stockage des métadonnées d'objet est faible.
Capacité disque de metrics faible	L'espace disponible pour la base de données de metrics est faible.
Faible stockage des données objet	L'espace disponible pour le stockage des données d'objet est faible.

Nom de l'alerte	Description
Remplacement du filigrane en lecture seule faible	Le remplacement du filigrane en lecture seule souple du volume de stockage est inférieur au filigrane optimisé minimum pour un nœud de stockage.
Capacité du disque racine faible	L'espace disponible sur le disque racine est faible.
Faible capacité des données système	L'espace disponible pour /var/local est faible. Si cette condition n'est pas résolue, les opérations S3 risquent d'échouer.
Petit répertoire tmp espace libre	L'espace disponible dans le répertoire /tmp est faible.

Alertes de réseau de nœuds ou de nœuds

Nom de l'alerte	Description
Le quorum de l'ADC n'est pas atteint	Le nœud de stockage avec le service ADC est hors ligne. Les opérations d'extension et de mise hors service sont bloquées jusqu'à ce que le quorum ADC soit rétabli.
Utilisation de la réception du réseau d'administration	L'utilisation de la réception sur le réseau d'administration est élevée.
Admin utilisation de la transmission réseau	L'utilisation de la transmission sur le réseau d'administration est élevée.
Échec de la configuration du pare-feu	Impossible d'appliquer la configuration du pare-feu.
Nœuds finaux de l'interface de gestion en mode de secours	Tous les terminaux de l'interface de gestion reviennent aux ports par défaut depuis trop longtemps.
Erreur de connectivité réseau du nœud	Des erreurs se sont produites lors du transfert des données entre les nœuds.
Erreur de trame de réception du réseau du nœud	Un pourcentage élevé des trames réseau reçues par un nœud a rencontré des erreurs.
Nœud non synchronisé avec le serveur NTP	Le nœud n'est pas synchronisé avec le serveur NTP (Network Time Protocol).
Nœud non verrouillé avec le serveur NTP	Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).
Réseau de nœuds non appliances arrêté	Un ou plusieurs périphériques réseau sont en panne ou déconnectés.

Nom de l'alerte	Description
Liaison de l'appliance de services vers le réseau d'administration	L'interface de l'appliance vers le réseau d'administration (eth1) est en panne ou déconnectée.
Interruption de la liaison de l'appliance de services sur le port réseau d'administration 1	Le port réseau Admin 1 de l'appliance est arrêté ou déconnecté.
Liaison de l'appliance de services vers le réseau client	L'interface de l'appliance vers le réseau client (eth2) est en panne ou déconnectée.
La liaison de l'appliance de services est inactive sur le port réseau 1	Le port réseau 1 de l'appliance est en panne ou déconnecté.
La liaison de l'appliance de services est inactive sur le port réseau 2	Le port réseau 2 de l'appliance est en panne ou déconnecté.
La liaison de l'appliance de services est inactive sur le port réseau 3	Le port réseau 3 de l'appliance est en panne ou déconnecté.
La liaison de l'appliance de services est inactive sur le port réseau 4	Le port réseau 4 de l'appliance est en panne ou déconnecté.
Liaison de l'appliance de stockage indisponible sur le réseau d'administration	L'interface de l'appliance vers le réseau d'administration (eth1) est en panne ou déconnectée.
Liaison du dispositif de stockage inactive sur le port réseau d'administration 1	Le port réseau Admin 1 de l'appliance est arrêté ou déconnecté.
La liaison de l'appliance de stockage sur le réseau client est inactive	L'interface de l'appliance vers le réseau client (eth2) est en panne ou déconnectée.
La liaison du dispositif de stockage est inactive sur le port réseau 1	Le port réseau 1 de l'appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 2	Le port réseau 2 de l'appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 3	Le port réseau 3 de l'appliance est en panne ou déconnecté.

Nom de l'alerte	Description
La liaison du dispositif de stockage est inactive sur le port réseau 4	Le port réseau 4 de l'apppliance est en panne ou déconnecté.
Le nœud de stockage n'est pas dans l'état de stockage souhaité	Le service LDR d'un nœud de stockage ne peut pas passer à l'état souhaité en raison d'une erreur interne ou d'un problème lié au volume
Utilisation de la connexion TCP	Le nombre de connexions TCP sur ce nœud est proche du nombre maximal de connexions pouvant être suivies.
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas, ou le nœud ne peut pas être atteint.
Redémarrage de nœud inattendu	Un nœud a été redémarré de manière inattendue au cours des 24 dernières heures.

Alertes sur les objets

Nom de l'alerte	Description
Échec de la vérification de l'existence de l'objet	Le travail de vérification de l'existence de l'objet a échoué.
La vérification de l'existence d'objet est bloquée	Le travail de vérification de l'existence de l'objet est bloqué.
Objets potentiellement perdus	Un ou plusieurs objets potentiellement perdus de la grille.
Objets orphelins détectés	Des objets orphelins ont été détectés.
La taille de la partie de l'envoi multipart S3 est trop grande	Un client tente une opération de téléchargement en plusieurs parties qui dépasse la limite de taille des parties.
S3 PLACEZ la taille de l'objet trop grande	Un client tente une opération PUT Object qui dépasse les limites de taille S3.
Requêtes S3 utilisant des en-têtes conditionnels non pris en charge	Un client S3 utilise des en-têtes conditionnels non pris en charge (If-Match ou If-None-Match) pour certaines opérations.
Requêtes S3 utilisant une région incorrecte avec l'espace de noms global activé	Un client S3 utilise la mauvaise région de signature pour accéder aux compartiments de cette grille.
Objet corrompu non identifié détecté	Un fichier a été trouvé dans le stockage objet répliqué qui n'a pas pu être identifié en tant qu'objet répliqué.

Alertes de corruption d'objets

Nom de l'alerte	Description
Incompatibilité de taille d'objet	Taille d'objet inattendue détectée lors de la procédure de vérification de l'existence de l'objet.

Alertes de services de plateforme

Nom de l'alerte	Description
Capacité des demandes en attente des services de plateforme faible	Le nombre de demandes de services de plateforme en attente approche de la capacité.
Services de plateforme non disponibles	Trop peu de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles sur un site.

Alertes de volume de stockage

Nom de l'alerte	Description
Le volume de stockage nécessite votre attention	Un volume de stockage est hors ligne et nécessite votre attention.
Le volume de stockage doit être restauré	Un volume de stockage a été restauré et doit être restauré.
Volume de stockage hors ligne	Un volume de stockage est hors ligne depuis plus de 5 minutes.
Tentative de remontage du volume de stockage	Un volume de stockage a été hors ligne et a déclenché un remontage automatique. Cela peut indiquer un problème de lecteur ou des erreurs de système de fichiers.
La restauration de volume n'a pas pu démarrer la réparation des données répliquées	La réparation des données répliquées pour un volume réparé n'a pas pu être démarrée automatiquement.

Alertes des services StorageGRID

Nom de l'alerte	Description
service nginx utilisant la configuration de sauvegarde	La configuration du service nginx n'est pas valide. La configuration précédente est maintenant utilisée.
le service nginx-gw utilise la configuration de sauvegarde	La configuration du service nginx-gw n'est pas valide. La configuration précédente est maintenant utilisée.

Nom de l'alerte	Description
Redémarrage requis pour désactiver FIPS	La politique de sécurité ne nécessite pas le mode FIPS, mais les modules FIPS sont utilisés.
Redémarrage requis pour activer FIPS	La politique de sécurité nécessite le mode FIPS, mais les modules FIPS ne sont pas utilisés.
Service SSH utilisant la configuration de sauvegarde	La configuration du service SSH n'est pas valide. La configuration précédente est maintenant utilisée.

Alertes aux locataires

Nom de l'alerte	Description
Utilisation élevée du quota par les locataires	Un pourcentage élevé de l'espace de quota est utilisé. Cette règle est désactivée par défaut car elle peut entraîner un trop grand nombre de notifications.

Métriques Prometheus couramment utilisées dans StorageGRID

Consultez cette liste de metrics Prometheus les plus utilisés pour mieux comprendre les conditions des règles d'alerte par défaut ou pour construire les conditions des règles d'alerte personnalisées.

Vous pouvez également [obtenez une liste complète de toutes les mesures](#).

Pour plus de détails sur la syntaxe des requêtes Prometheus, voir "[Principes de base des requêtes](#)".

Quels sont les metrics Prometheus ?

Les metrics Prometheus sont des mesures de séries chronologiques. Le service Prometheus sur les nœuds d'administration collecte ces metrics à partir des services sur tous les nœuds. Des metrics sont stockés sur chaque nœud d'administration jusqu'à ce que l'espace réservé aux données Prometheus soit plein. Lorsque le `/var/local/mysql_ibdata/` volume atteint sa capacité, les mesures les plus anciennes sont supprimées en premier.

Où sont utilisés les metrics Prometheus ?

Les metrics collectées par Prometheus sont utilisés à plusieurs endroits dans Grid Manager :

- **Page noeuds** : les graphiques et graphiques des onglets disponibles sur la page noeuds utilisent l'outil de visualisation Grafana pour afficher les metrics de séries chronologiques recueillies par Prometheus. Grafana affiche les données de séries chronologiques aux formats graphique et graphique, tandis que Prometheus sert de source de données back-end.



- **Alertes** : les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte qui utilisent des metrics Prometheus sont définies comme vraies.
- **Grid Management API** : vous pouvez utiliser des metrics Prometheus dans des règles d'alerte personnalisées ou avec des outils d'automatisation externes pour surveiller votre système StorageGRID. La liste complète des metrics de Prometheus est disponible via l'API Grid Management. (En haut de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **documentation API > metrics**.) Bien que plus d'un millier de mesures soient disponibles, seul un nombre relativement faible est requis pour surveiller les opérations StorageGRID les plus stratégiques.



Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

- La page **Support > 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 fonctions et options de menu de la page métriques sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications.

Liste des mesures les plus courantes

La liste suivante répertorie les metrics Prometheus les plus utilisés.



Les indicateurs incluant *private* dans leur nom sont destinés à un usage interne uniquement et sont susceptibles d'être modifiés sans préavis entre les versions de StorageGRID.

alertmanager_notifications_failed_total

Nombre total de notifications d'alerte ayant échoué.

node_filesystem_dispo_octets

Espace système de fichiers disponible pour les utilisateurs non root en octets.

Node_Memory_MemAvailable_Bytes

Champ informations mémoire MemAvailable_Bytes.

node_network_carrier

Valeur porteuse de `/sys/class/net/iface`.

node_network_recy_errs_total

Statistiques du périphérique réseau `receive_errs`.

node_network_transmit_errs_total

Statistiques du périphérique réseau `transmit_errs`.

storagegrid_panne_administrative

Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau.

storagegrid_appliance_compute_controller_status

L'état du matériel du contrôleur de calcul d'une appliance.

disques_défaillants_appliance_storagegrid

Pour le contrôleur de stockage d'une appliance, le nombre de disques qui ne sont pas optimaux.

état_matériel_contrôleur_stockage_appliance_storagegrid

État global du matériel du contrôleur de stockage d'une appliance.

conteneurs_contenu_seaux_et_conteneurs_storagegrid

Le nombre total de buckets S3 connus par ce nœud de stockage.

objets_contenu_storagegrid

Le nombre total d'objets de données S3 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.

objet_contenu_storagegrid_perdu

Le nombre total d'objets détectés par ce service est manquant dans le système StorageGRID. Des mesures doivent être prises pour déterminer la cause de la perte et si la récupération est possible.

["Dépanner les données d'objet perdues ou manquantes"](#)

storagegrid_http_sessions_entrant_tenté

Nombre total de sessions HTTP ayant été tentées vers un nœud de stockage.

storagegrid_http_sessions_entrant_actuellement_établi

Nombre de sessions HTTP actuellement actives (ouvertes) sur le nœud de stockage.

storagegrid_http_sessions_incoming_failed

Nombre total de sessions HTTP qui n'ont pas réussi à se terminer correctement, soit en raison d'une requête HTTP mal formée, soit en cas d'échec du traitement d'une opération.

storagegrid_http_sessions_entrant_réussi

Nombre total de sessions HTTP terminées avec succès.

objets_ilm_en_attente_arrière-plan

Le nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir de l'analyse.

storagegrid_ilm_en_attente_client_évaluation_objets_par_seconde

Vitesse actuelle d'évaluation des objets par rapport à la règle ILM de ce nœud.

objet_client_attente_ilm_en_attente

Le nombre total d'objets de ce nœud attend l'évaluation ILM des opérations client (par exemple, ingestion).

objets_ilm_en_attente_total_storagegrid

Le nombre total d'objets en attente d'évaluation ILM.

ilm_scan_objets_par_seconde

Vitesse à laquelle les objets appartenant à ce nœud sont analysés et mis en file d'attente d'ILM.

storagegrid_ilm_scan_perce_estimé_minutes

Durée estimée d'une analyse ILM complète sur ce nœud.

Remarque : Une analyse complète ne garantit pas que ILM a été appliquée à tous les objets appartenant à ce nœud.

storagegrid_load_balancer_cert_exexpiration_time

Le temps d'expiration du certificat de nœud final de l'équilibreur de charge en secondes depuis l'époque.

storagegrid_metadata_requêtes_moyenne_latence_millisecondes

Temps moyen requis pour exécuter une requête sur le magasin de métadonnées via ce service.

storagegrid_réseau_reçu_octets

Quantité totale de données reçues depuis l'installation.

octets_réseau_transmis_storagegrid

Quantité totale de données envoyées depuis l'installation.

pourcentage_utilisation_cpu_storagegrid_nœud_nœud

Pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique le niveau d'occupation du service. Le temps CPU disponible dépend du nombre de CPU du serveur.

storagegrid_ntp_choisi_source_temps_offset_millisecondes

Décalage systématique du temps fourni par une source de temps choisie. Le décalage est introduit lorsque le délai d'accès à une source de temps n'est pas égal au temps requis pour que la source de temps atteigne le client NTP.

storagegrid_ntp_verrouillé

Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

Quantité totale de données ingérées à partir des clients S3 pour ce nœud de stockage, depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_data_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

Le nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec d'autorisation S3.

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 à la suite d'un échec d'autorisation.

storagegrid_servercertificate_management_interface_cert_expiration_days

Nombre de jours avant l'expiration du certificat de l'interface de gestion.

storagegrid_servercertificate_storage_api_endpoints_cert_expiration_days

Nombre de jours avant l'expiration du certificat de l'API de stockage objet.

storagegrid_service_cpu_secondes

Durée cumulée pendant laquelle le CPU a été utilisé par ce service depuis l'installation.

octets_usage_mémoire_service_storagegrid

La quantité de mémoire (RAM) actuellement utilisée par ce service. Cette valeur est identique à celle affichée par l'utilitaire Linux TOP sous RES.

octets_réseau_service_storagegrid_reçus_netapp

Quantité totale de données reçues par ce service depuis l'installation.

octets_réseau_service_storagegrid_transmis_netapp

Quantité totale de données envoyées par ce service.

redémarrages_service_storagegrid

Nombre total de fois où le service a été redémarré.

storagegrid_service_runtime_seconds

Durée totale d'exécution du service depuis l'installation.

temps_disponibilité_service_storagegrid_secondes

Durée totale d'exécution du service depuis son dernier redémarrage.

storage_state_current_storagegrid

État actuel des services de stockage. Les valeurs d'attribut sont :

- 10 = hors ligne
- 15 = entretien
- 20 = lecture seule
- 30 = en ligne

état_stockage_storage_storagegrid

État actuel des services de stockage. Les valeurs d'attribut sont :

- 0 = aucune erreur

- 10 = en transition
- 20 = espace libre insuffisant
- 30 = Volume(s) indisponible
- 40 = erreur

storagegrid_utilisation_données_octets

Estimation de la taille totale des données d'objet répliquées et codées d'effacement sur le nœud de stockage.

storage_utilisation_métadonnées_autorisés_storagegrid_octets

Espace total sur le volume 0 de chaque nœud de stockage autorisé pour les métadonnées d'objet. Cette valeur est toujours inférieure à l'espace réel réservé aux métadonnées sur un nœud, car une partie de l'espace réservé est requise pour les opérations essentielles de base de données (telles que la compaction et la réparation) et les futures mises à niveau matérielles et logicielles. l'espace autorisé pour les métadonnées de l'objet contrôle la capacité globale des objets.

octets_métadonnées_utilisation_stockage_storagegrid

Volume des métadonnées d'objet sur le volume de stockage 0, en octets.

storage_usage_total_octets_espace_stockage_storagegrid

Quantité totale d'espace de stockage alloué à tous les magasins d'objets.

octets_stockage_utilisation_de_stockage_utilisables_storagegrid

Quantité totale d'espace de stockage objet restant. Calculé en ajoutant ensemble la quantité d'espace disponible pour tous les magasins d'objets du nœud de stockage.

octets_données_utilisation_storagegrid_tenant

Taille logique de tous les objets pour le locataire.

nombre_d'objets_usage_storagegrid_tenant_storagegrid

Le nombre d'objets pour le locataire.

octets_quota_utilisation_storagegrid_tenant_octets

Quantité maximale d'espace logique disponible pour les objets du locataire. Si aucune mesure de quota n'est fournie, une quantité illimitée d'espace est disponible.

Obtenez une liste de toutes les mesures

pour obtenir la liste complète des mesures, utilisez l'API de gestion de grille.

Étapes

1. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
2. Localisez les opérations **métriques**.
3. Exécutez `GET /grid/metric-names` l'opération.
4. Téléchargez les résultats.

Référence des fichiers journaux

Fichiers journaux StorageGRID

StorageGRID fournit des journaux utilisés pour capturer les événements, les messages de diagnostic et les conditions d'erreur. Il se peut que vous soyez invité à collecter les fichiers journaux et à les transférer au support technique pour faciliter le dépannage.

Les journaux sont classés comme suit :

- ["Journaux du logiciel StorageGRID"](#)
- ["Journaux de déploiement et de maintenance"](#)
- ["Sur le bycast.log"](#)



Les détails fournis pour chaque type de journal sont fournis à titre de référence uniquement. Les journaux sont destinés au dépannage avancé par le support technique. Les techniques avancées qui impliquent la reconstruction de l'historique des problèmes à l'aide des journaux d'audit et des fichiers journaux de l'application sont hors de portée de ces instructions.

Accéder aux journaux

Pour accéder aux journaux, vous pouvez ["collecter les fichiers journaux et les données système"](#) à partir d'un ou plusieurs nœuds sous forme d'archive de fichier journal unique. Ou, vous pouvez accéder aux fichiers journaux individuels pour chaque nœud de grille comme suit :

Étapes

1. Entrez la commande suivante : `ssh admin@grid_node_IP`
2. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
3. Entrez la commande suivante pour basculer en root : `su -`
4. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Exportez 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.
- Meilleure visibilité sur les requêtes S3 qui renvoient des erreurs, sans l'impact sur les performances que provoquent les méthodes de journalisation des audits.
- Accès aux requêtes de couche HTTP et aux codes d'erreur faciles à analyser.
- Meilleure visibilité sur les demandes bloquées par les classificateurs du trafic au niveau de l'équilibreur de charge.

Pour exporter les journaux, reportez-vous à ["Configurer la gestion des journaux et le serveur syslog externe"](#) .

Catégories de fichiers journaux

L'archive du fichier journal StorageGRID contient les journaux décrits pour chaque catégorie et les fichiers supplémentaires contenant des mesures et la sortie de la commande debug.

Emplacement d'archivage	Description
acct-tunnel.log	Journal de l'assistant de tunnel de compte qui fonctionne avec le répartiteur de charge.
audit	Messages d'audit générés pendant le fonctionnement normal du système.
base-os-logs	Informations sur le système d'exploitation de base, notamment les versions d'images StorageGRID.
packs	Informations de configuration globale (bundles).
service de cache	Journaux du service de cache (uniquement sur les nœuds de passerelle).
cassandra	Informations sur la base de données Cassandra et journaux de réparation de couches.
d'europe	Informations VCS sur le nœud actuel et les informations de groupe EC par ID de profil.
grille	Journaux de grille généraux, y compris débogage (<code>broadcast.log</code>) et <code>servermanager</code> journaux.
grid.json	Le fichier de configuration du grid est partagé sur tous les nœuds. En outre, <code>node.json</code> est spécifique au nœud actuel.
hagroups	Metrics et journaux pour les groupes de haute disponibilité.
installer	<code>Gdu-server</code> et installez les journaux.
internal-access.log	Journal du trafic du proxy HTTP interne.
Lambda-arbitre	Journaux associés à la demande de proxy S3 Select.
fuite	Journaux du service leakd.
lumberjack.log	Messages de débogage liés à la collecte de journaux.
manage-audit.log	<code>mgmt-api</code> accéder aux journaux d'audit.
Métriques	Journaux de service pour Grafana, Jaeger, node exportateur et Prometheus.
etcd	Journaux d'accès divers et d'erreurs.
mysql	La configuration de la base de données MariaDB et les journaux associés.

Emplacement d'archivage	Description
nette	Journaux générés par des scripts de mise en réseau et le service Dynap.
nginx	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération du grid. Inclut également les journaux de trafic Grid Manager et tenant Manager.
nginx-gw	• <code>access.log</code>: Le gestionnaire de grille et le gestionnaire de locataires demandent des messages de journal. ◦ Ces messages sont préfixés avec lorsqu'ils sont <code>mgmt</code> : exportés à l'aide de syslog. ◦ 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 entrantes de la grille transversale. ◦ Ces messages sont préfixés avec lorsqu'ils sont <code>cgr</code> : exportés à l'aide de syslog. ◦ 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 demande aux points de terminaison de l'équilibreur de charge. ◦ Ces messages sont préfixés avec lorsqu'ils sont <code>endpoint</code> : exportés à l'aide de syslog. ◦ 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>: Lié à la nouvelle alerte de vérification DNS. • <code>stream-access.log</code> : sessions proxy de flux TCP/TLS (couche 4) pour le bloc de flux. Remarque : Ceci n'est pas un journal de requêtes HTTP.
ntp	Fichier de configuration et journaux NTP.
Objets orphelins	Journaux relatifs aux objets orphelins.
os	Fichier d'état de nœud et de grille, y compris les services <code>pid</code> .

Emplacement d'archivage	Description
autre	Les fichiers journaux sous <code>/var/local/log</code> qui ne sont pas collectés dans d'autres dossiers.
diminution des	Informations de performances pour le CPU, la mise en réseau et les E/S de disque
données prometheus	Metrics Prometheus actuels si la collecte des journaux inclut des données Prometheus.
provisionnement	Journaux relatifs au processus de provisionnement de la grille.
radeau	Journaux de grappe raft utilisés dans les services de plate-forme.
revision_history.json	Historique des révisions.
routed-s3-access.log.gz	Journal d'accès pour le trafic de fédération de grille acheminé comme S3 (espace de noms global/URL de fédération).
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 des sockets pour le débogage réseau.
system-bucket.log	<code>update-system-bucket-configuration.log</code> : Journaux du compartiment système.
system-commands.txt	Résultat des commandes du conteneur StorageGRID. Contient des informations sur le système, telles que la mise en réseau et l'utilisation du disque.
synchroniser-package-récupération	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.
update-cipher-configurations.log	<code>update-cors-configurations.log</code> : Journaux de traces relatifs aux modifications TLS/chiffrements et CORS.
update-leakd-configurations.log	Journal de configuration de la détection des orphelins.

Journaux du logiciel StorageGRID

Les journaux StorageGRID vous permettent de résoudre les problèmes.



Si vous souhaitez envoyer vos journaux à un serveur syslog externe ou modifier la destination des informations d'audit telles que le `broadcast.log` et `nms.log`, voir "[Configurer la gestion des journaux](#)".

Journaux StorageGRID généraux

Nom du fichier	Remarques	Ci-après
<code>/var/local/log/broadcast.log</code>	Le fichier de dépannage principal de StorageGRID.	Tous les nœuds
<code>/var/local/log/broadcast-err.log</code>	Contient un sous-ensemble de <code>broadcast.log</code> (messages de gravité ERREUR et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système.	Tous les nœuds
<code>/var/local/core/</code>	Contient tous les fichiers core dump créés si le programme se termine anormalement. Les causes possibles sont les échecs d'assertion, les violations ou les retards de thread. Remarque : le fichier <code>/var/local/core/kexec_cmd</code> existe généralement sur les nœuds de l'appliance et n'indique pas d'erreur.	Tous les nœuds

Journaux liés au chiffrement

Nom du fichier	Remarques	Ci-après
<code>/var/local/log/ssh-config-generation.log</code>	Contient des journaux relatifs à la génération de configurations SSH et au rechargement de services SSH.	Tous les nœuds
<code>/var/local/log/nginx/config-generation.log</code>	Contient les journaux relatifs à la génération des configurations nginx et au rechargement des services nginx.	Tous les nœuds
<code>/var/local/log/nginx-gw/config-generation.log</code>	Contient les journaux relatifs à la génération des configurations nginx-gw (et au rechargement des services nginx-gw).	Nœuds d'administration et de passerelle
<code>/var/local/log/update-cipher-configurations.log</code>	Contient des journaux relatifs à la configuration des règles TLS et SSH.	Tous les nœuds

Journaux de fédération du grid

Nom du fichier	Remarques	Ci-après
/var/local/log/update_grid_federation_config.log	Contient les journaux relatifs à la génération des configurations nginx et nginx-gw pour les connexions de fédération de grille.	Tous les nœuds

Journaux NMS

Nom du fichier	Remarques	Ci-après
/var/local/log/nms.log	• Capture des notifications à partir du Grid Manager et du tenant Manager. • Capture les événements liés au fonctionnement du service NMS. Par exemple, les notifications par e-mail et les modifications de configuration. • Contient des mises à jour de bundle XML résultant des modifications de configuration effectuées dans le système. • Contient des messages d'erreur liés au sous-échantillonnage de l'attribut effectué une fois par jour. • Contient les messages d'erreur du serveur Web Java, par exemple les erreurs de génération de page et les erreurs HTTP Status 500. • Contient des journaux liés à AutoSupport.	Nœuds d'administration
/var/local/log/nms.errlog	Contient des messages d'erreur relatifs aux mises à niveau de la base de données MySQL. Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds d'administration
/var/local/log/nms.requestlog	Contient des informations sur les connexions sortantes de l'API de gestion vers les services StorageGRID internes.	Nœuds d'administration

Journaux Server Manager

Nom du fichier	Remarques	Ci-après
/var/local/log/servermanager.log	Fichier journal de l'application Server Manager exécutée sur le serveur.	Tous les nœuds
/Var/local/log/GridstatBackend.errlog	Fichier journal de l'application back-end de l'interface utilisateur graphique de Server Manager.	Tous les nœuds
/var/local/log/gridstat.errlog	Fichier journal de l'interface graphique de Server Manager.	Tous les nœuds

Journaux des services StorageGRID

Nom du fichier	Remarques	Ci-après
/var/local/log/acct.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/adc.errlog	Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds de stockage exécutant le service ADC
/var/local/log/ams.errlog		Nœuds d'administration
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Journaux du service de cache.	Nœuds de passerelle
/var/local/log/cassandra/system.log	Informations pour le magasin de métadonnées (base de données Cassandra) pouvant être utilisées en cas de problème lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation nodetool cale.	Nœuds de stockage
/var/local/log/cassandra-reaper.log	Informations concernant le service Cassandra Reaper, qui répare les données de la base de données Cassandra.	Nœuds de stockage
/var/local/log/cassandra-reaper.errlog	Informations d'erreur pour le service Cassandra Reaper.	Nœuds de stockage
/var/local/log/chunk.errlog		Nœuds de stockage

Nom du fichier	Remarques	Ci-après
/var/local/log/cmn.errlog		Nœuds d'administration
/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/dylog*	Contient des journaux liés au service dynap, qui surveille la grille pour les modifications IP dynamiques et met à jour la configuration locale.	Tous les nœuds
/var/local/log/grafana.log	Journal associé au service Grafana, utilisé pour la visualisation des metrics dans Grid Manager.	Nœuds d'administration
/var/local/log/hagroups.log	Journal associé aux groupes haute disponibilité.	Nœuds d'administration et nœuds de passerelle
/var/local/log/hagroups_events.log	Suivi des changements d'état, tels que la transition de LA SAUVEGARDE vers LE MAÎTRE ou LE DÉFAUT.	Nœuds d'administration et nœuds de passerelle
/var/local/log/idnt.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/jaeger.log	Journal associé au service jaeger, qui est utilisé pour la collecte de traces.	Tous les nœuds
/var/local/log/kstn.errlog		Nœuds de stockage exécutant le service ADC

Nom du fichier	Remarques	Ci-après
/var/local/log/lambda*	Contient les journaux du service S3 Select.	Nœuds d'administration et de passerelle Seuls certains nœuds d'administration et de passerelle contiennent ce journal. Voir la "Exigences et limitations de S3 Select pour les nœuds d'administration et de passerelle" .
/var/local/log/ldr.errlog		Nœuds de stockage
/var/local/log/miscd/*.log	Contient des journaux pour le service MISCd (démon de contrôle du service d'information), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, comme interroger l'état des services s'exécutant sur d'autres nœuds.	Tous les nœuds
/var/local/log/nginx/*.log	Contient des journaux pour le service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de réseau (comme Prometheus et Dynap) pour pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
/var/local/log/nginx-gw/*.log	Contient les journaux généraux relatifs au service nginx-gw, y compris les journaux d'erreurs et les journaux des ports d'administration restreints sur les nœuds d'administration.	Nœuds d'administration et nœuds de passerelle
/var/local/log/nginx-gw/cgr-access.log.gz	Contient des journaux d'accès relatifs au trafic de réplication inter-grid.	Nœuds d'administration, nœuds de passerelle ou les deux, en fonction de la configuration de fédération grid. Uniquement disponible sur la grille de destination pour la réplication inter-grid.

Nom du fichier	Remarques	Ci-après
/var/local/log/nginx-gw/endpoint-access.log.gz	Contient les journaux d'accès du service Load Balancer, qui assure l'équilibrage de la charge du trafic S3 entre les clients et les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
/var/local/log/persistence*	Contient les journaux du service Persistence, qui gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage.	Tous les nœuds
/var/local/log/prometheus.log	Pour tous les nœuds, il contient le journal de service de l'exportateur de nœuds et le journal des services de metrics de l'outil d'exportation de nœuds. Pour les nœuds d'administration, contient également les journaux des services Prometheus et Alert Manager.	Tous les nœuds
/var/local/log/raft.log	Contient la sortie de la bibliothèque utilisée par le service RSM pour le protocole de radeau.	Nœuds de stockage avec service RSM
/var/local/log/rms.errlog	Contient les journaux du service RSM (State machine Service) répliqué, qui est utilisé pour les services de plateforme S3.	Nœuds de stockage avec service RSM
/var/local/log/ssm.errlog		Tous les nœuds
/var/local/log/update-s3vs-domains.log	Contient des journaux relatifs aux mises à jour de traitement pour la configuration des noms de domaine hébergés sur des serveurs virtuels S3. consultez les instructions d'implémentation des applications client S3.	Nœuds d'administration et de passerelle
/var/local/log/update-snmp-firewall.*	Contiennent des journaux relatifs aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
/var/local/log/update-sysl.log	Contient des journaux relatifs aux modifications apportées à la configuration syslog du système.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
/var/local/log/update-traffic-classes.log	Contient des journaux relatifs aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
/var/local/log/update-utcn.log	Contient des journaux liés au mode réseau client non fiable sur ce nœud.	Tous les nœuds

Informations associées

- ["Sur le bycast.log"](#)
- ["UTILISEZ L'API REST S3"](#)

Journaux de déploiement et de maintenance dans StorageGRID

Vous pouvez utiliser les journaux de déploiement et de maintenance pour résoudre les problèmes.

Nom du fichier	Remarques	Ci-après
/var/local/log/install.log	Créé lors de l'installation du logiciel. Contient un enregistrement des événements d'installation.	Tous les nœuds
/var/local/log/expansion-progress.log	Créé pendant les opérations d'extension. Contient un enregistrement des événements d'extension.	Nœuds de stockage
/var/local/log/pa-move.log	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
/var/local/log/pa-move-new_pa.log	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
/var/local/log/pa-move-old_pa.log	Créé lors de l'exécution <code>pa-move.sh</code> du script.	Nœud d'administration principal
/var/local/log/gdu-server.log	Créé par le service GDU. Contient les événements liés aux procédures d'approvisionnement et de maintenance gérées par le nœud d'administration principal.	Nœuds d'administration
/var/local/log/send_admin_hw.log	Créé lors de l'installation. Contient des informations de débogage liées aux communications d'un nœud avec le nœud d'administration principal.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
/var/local/log/upgrade.log	Créé lors de la mise à niveau logicielle. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

En savoir plus sur le fichier bycast.log de StorageGRID

Le fichier est le fichier `/var/local/log/bycast.log` de dépannage principal du logiciel StorageGRID. Il existe un `bycast.log` fichier pour chaque nœud de grille. Le fichier contient des messages spécifiques à ce nœud de grille.

Le fichier `/var/local/log/bycast-err.log` est un sous-ensemble de `bycast.log`. Il contient des messages D'ERREUR de gravité et D'ERREUR CRITIQUE.

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 la gestion des journaux et le serveur syslog externe"](#).

Rotation des fichiers pour bycast.log

Lorsque le `bycast.log` fichier atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal démarre.

Le fichier enregistré est renommé `bycast.log.1` et le nouveau fichier est nommé `bycast.log`. Lorsque le nouveau `bycast.log` atteint 1 Go, `bycast.log.1` est renommé et compressé pour devenir `bycast.log.2.gz`, et `bycast.log` est renommé `bycast.log.1`.

La limite de rotation pour `bycast.log` est de 21 fichiers. Lorsque la 22e version du `bycast.log` fichier est créée, le fichier le plus ancien est supprimé.

La limite de rotation pour `bycast-err.log` est de sept fichiers.



Si un fichier journal a été compressé, vous ne devez pas le décompresser au même emplacement que celui dans lequel il a été écrit. La décompression du fichier au même emplacement peut interférer avec les scripts de rotation du journal.

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 la gestion des journaux et le serveur syslog externe"](#).

Informations associées

["Collecte de fichiers journaux et de données système"](#)

Messages en bycast.log

Les 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 la grille.

Exemple de message ADE :

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685      0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

Les messages ADE contiennent les informations suivantes :

Segment de message	Valeur dans l'exemple
ID du nœud	12455685
ID processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	EVHR
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUU)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Messagerie	SVMR : le bilan de santé du volume 3 a échoué avec la raison « tout »

Gravité des messages en `broadcast.log`

Des niveaux de sévérité sont attribués aux messages `broadcast.log` de la section.

Par exemple :

- **AVIS** — un événement qui devrait être enregistré s'est produit. La plupart des messages du journal sont à ce niveau.
- **AVERTISSEMENT** — une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite qui aura une incidence sur les opérations.
- **CRITIQUE** — une condition anormale s'est produite qui a arrêté les opérations normales. Vous devez immédiatement corriger la condition sous-jacente.

Codes d'erreur dans `broadcast.log`

La plupart des messages d'erreur de la `broadcast.log` contiennent des codes d'erreur.

Le tableau suivant répertorie les codes non numériques courants dans la `broadcast.log` signification exacte d'un code non numérique dépend du contexte dans lequel il est signalé.

Code d'erreur	Signification
CAN	Pas d'erreur
GERR	Inconnu
ANNUL	Annulée
ABRT	Abandonné
TOUT	Délai dépassé
INVL	Non valide
NFND	Introuvable
VERS	Version
CONF	Configuration
ECHEC	Échec
CIPD	Incomplet
L'A FAIT	L'a fait
SUNV	Service indisponible

Le tableau suivant répertorie les codes d'erreur numériques dans `bycast.log`.

Numéro de l'erreur	Code d'erreur	Signification
001	EPERM	Opération non autorisée
002	RÉF	Ce fichier ou répertoire n'est pas disponible
003	ESRCH	Pas de tel processus
004	EINTA	Appel système interrompu
005	EIO	Erreur d'E/S.
006	ENXIO	Ce périphérique ou cette adresse n'est pas disponible

Numéro de l'erreur	Code d'erreur	Signification
007	E2BIG	Liste d'arguments trop longue
008	ENOEXEC	Erreur de format Exec
009	EBADF	Numéro de fichier incorrect
010	ECHILD	Aucun processus enfant
011	EAGAIN	Réessayez
012	ENOMEM	Mémoire insuffisante
013	EACCES	Autorisation refusée
014	PAR DÉFAUT	Adresse incorrecte
015	ENOTBLK	Dispositif de blocage requis
016	EBUSY	Périphérique ou ressource occupé
017	EEXIST	Le fichier existe déjà
018	EXDEV	Liaison interpériphérique
019	ENV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	Est un répertoire
022	EINVAL	Argument non valide
023	PAGE D'ACCUEIL	Dépassement de la table de fichiers
024	EMFILE	Trop de fichiers ouverts
025	EN COURS	Pas une machine à écrire
026	ETXTBBY	Fichier texte occupé
027	EFBIG	Fichier trop volumineux

Numéro de l'erreur	Code d'erreur	Signification
028	ENOSPC	Il n'y a plus d'espace sur l'appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule
031	ALINK	Trop de liens
032	EPIPE	Tuyau cassé
033	ÉDOM	Argument mathématique hors domaine de la fonction
034	ERANGE	Résultat mathématique non représentativité
035	EDEADLE	L'impasse de la ressource se produirait
036	ENAMETOOLONG	Nom de fichier trop long
037	ENOLCK	Aucun verrouillage d'enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ENOTEMPTY	Répertoire non vide
040	ELOP	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identificateur supprimé
044	ECHNG	Numéro de canal hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté
047	EL3RST	Remise à zéro du niveau 3
048	ELNRNG	Numéro de liaison hors plage

Numéro de l'erreur	Code d'erreur	Signification
049	EUNATCH	Pilote de protocole non connecté
050	ENOCSI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté
052	EBADE	Échange non valide
053	ADR	Descripteur de demande non valide
054	EXFULL	Exchange complet
055	ENOANO	Pas d'anode
056	EBADRQC	Code de demande non valide
057	EBADSLT	Emplacement non valide
058		
059	EBFONT	Format de fichier de police incorrect
060	ENOSTR	Le périphérique n'est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Temporisation expirée
063	ENOSR	Ressources hors flux
064	ENONET	La machine n'est pas sur le réseau
065	ENOPKG	Package non installé
066	EREMOTE	L'objet est distant
067	LIAISON	Le lien a été rompu
068	EADV	Erreur de publicité
069	ESRMNT	Erreur Srmount

Numéro de l'erreur	Code d'erreur	Signification
070	ECOMM	Erreur de communication sur l'envoi
071	EPROTO	Erreur de protocole
072	EMULTIHOP	Multihop tenté
073	EDOTTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	EOVERFLOW	Valeur trop élevée pour le type de données défini
076	ENOTUNIQ	Nom non unique sur le réseau
077	EDFD	Descripteur de fichier dans un état incorrect
078	SOUS-GROUPE	Adresse distante modifiée
079	ELIBACC	Impossible d'accéder à une bibliothèque partagée nécessaire
080	ELIBBAD	Accès à une bibliothèque partagée endommagée
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ELIBEXEC	impossible d'exécuter directement une bibliothèque partagée
084	EILSEQ	Séquence d'octets non autorisée
085	SYSTÈME	L'appel système interrompu doit être redémarré
086	ESTRPIPE	Erreur de tuyau de flux
087	EUSERS	Trop d'utilisateurs
088	ENOTSOCK	Fonctionnement de la prise femelle sur non prise femelle
089	EDESTADDRREQ	Adresse de destination requise

Numéro de l'erreur	Code d'erreur	Signification
090	EMSGSIZE	Message trop long
091	EPROTOTYPE	Type de protocole incorrect pour le socket
092	EN OPTION	Protocole non disponible
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le terminal de transport
096	EPFNOSUPPORT	Famille de protocoles non prise en charge
097	EAFNOSUPPORT	Famille d'adresses non prise en charge par le protocole
098	EADDRINUSE	Adresse déjà utilisée
099	EADDRNOTAVAIL	Impossible d'attribuer l'adresse demandée
100	EN-TÊTE	Le réseau ne fonctionne pas
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion au réseau a été interrompue en raison d'une réinitialisation
103	ECONNABORTED	Le logiciel a provoqué l'arrêt de la connexion
104	ECONRESET	Réinitialisation de la connexion par poste
105	ENOBUFS	Aucun espace tampon disponible
106	EISCONN	Terminal de transport déjà connecté
107	ENOTCONN	Le terminal de transport n'est pas connecté
108	ESHUTDOWN	Impossible d'envoyer après l'arrêt du terminal de transport
109	ETOONYREFS	Trop de références : impossible d'épisser

Numéro de l'erreur	Code d'erreur	Signification
110	ETIMDOUT	La connexion a expiré
111	ECONREFUSED	Connexion refusée
112	EHOSTDOWN	L'hôte n'est pas en panne
113	EHOSTUNREACH	Aucune route vers l'hôte
114	EALREADY	Opération déjà en cours
115	EINPROGRESS	Opération en cours
116		
117	EUCLEAN	La structure doit être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAIL	Aucun sémaphores XENIX n'est disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTIO	Erreur d'E/S distante
122	EDUQUOT	Quota dépassé
123	ENOMEDIUM	Aucun support trouvé
124	EMEDIUMTYPE	Type de support incorrect
125	ECANCELED	Opération annulée
126	ENOKAY	Clé requise non disponible
127	EKEYEXPIRED	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	EOWNERDEAD	Pour des mutexes robustes : le propriétaire est mort

Numéro de l'erreur	Code d'erreur	Signification
131	ENOTRECOVERABLE	Pour les mutexes robustes : état non récupérable

Configurer la gestion des journaux et le serveur syslog externe

Serveurs syslog externes dans StorageGRID

Un serveur syslog externe est un serveur hors de StorageGRID que vous pouvez utiliser pour collecter les informations d'audit système sur un emplacement unique. L'utilisation d'un serveur syslog externe vous permet de réduire le trafic réseau sur vos nœuds d'administration et de gérer les informations plus efficacement. Pour StorageGRID, le format de paquet de messages syslog sortants est conforme à la norme RFC 3164.

Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe sont les suivants :

- Journaux d'audit contenant les messages d'audit générés pendant le fonctionnement normal du système
- Événements liés à la sécurité tels que les connexions et la remontée à la racine
- Fichiers journaux d'application pouvant être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème rencontré

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'applications et les événements de sécurité.
- Réduisez le trafic réseau sur vos nœuds d'administration, car les informations d'audit sont transférées directement depuis les différents nœuds de stockage vers le serveur syslog externe, sans devoir 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 communes des implémentations de serveur syslog externe.



Pour optimiser les options de restauration complète des données en cas de défaillance du serveur syslog externe, jusqu'à 20 Go de journaux locaux d'enregistrements d'audit (`localaudit.log`) sont conservés sur chaque nœud.

Comment configurer un serveur syslog externe

Pour savoir comment configurer un serveur syslog externe, consultez ["Configurer la gestion des journaux 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 d'autorité de certification du serveur** : un ou plusieurs certificats d'autorité de certification de confiance pour vérifier le serveur syslog externe dans le codage PEM. Si omis, le certificat d'autorité de certification de la grille par défaut sera utilisé.
- **Certificat client** : certificat client pour l'authentification au serveur syslog externe dans le codage PEM.
- **Clé privée client** : clé privée pour le certificat client dans le codage PEM.



Si vous utilisez un certificat client, vous devez également utiliser une clé privée client. Si vous fournissez une clé privée chiffrée, vous devez également fournir la phrase de passe. L'utilisation d'une clé privée chiffrée n'est pas un avantage majeur en matière de sécurité, car la clé et la phrase de passe doivent être stockées. Si elles sont disponibles, il est recommandé de recourir à une clé privée non chiffrée pour plus de simplicité.

Comment estimer la taille du serveur syslog externe

En principe, la taille de la grille est adaptée au débit requis, défini en termes d'opérations S3 par seconde ou d'octets par seconde. Par exemple, votre grid peut être capable de gérer 1,000 opérations S3 par seconde ou 2,000 Mo par seconde, d'ingales et de récupérations d'objets. Il est conseillé de dimensionner votre serveur syslog externe en fonction des besoins de votre grid.

Cette section fournit des formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types requis par votre serveur syslog externe en termes de caractéristiques de performance connues ou souhaitées de la grille (opérations S3 par seconde).

Utilisez des opérations S3 par seconde dans les formules d'estimation

Si votre grille a été dimensionnée pour un débit exprimé en octets par seconde, vous devez convertir ce dimensionnement en opérations S3 par seconde afin d'utiliser les formules d'estimation. Pour convertir le débit du grid, vous devez d'abord déterminer la taille d'objet moyenne que vous pouvez utiliser les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utilisent StorageGRID. Par exemple, si la taille du grid a été dimensionnée pour atteindre un débit de 2,000 Mo/seconde, et que la taille d'objet moyenne est de 2 Mo, votre grille a été dimensionnée pour traiter 1,000 opérations S3 par seconde (2,000 Mo/2 Mo).



Les formules de dimensionnement externe du serveur syslog présentées dans les sections suivantes fournissent des estimations communes (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, un taux plus élevé ou moins élevé de messages syslog ou de données syslog peut être constaté que les formules le prévoient. Les formules sont destinées à être utilisées uniquement comme directives.

Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille doit prendre en charge, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes : Dans l'hypothèse où vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,000 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux de 1.6 Mo par seconde.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'audit, les variables supplémentaires les plus importantes sont le pourcentage d'opérations S3 PUT (vs. Gets) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs de journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Nous allons utiliser P pour représenter le pourcentage d'opérations S3 qui sont PUT, où $0 \leq P \leq 1$ (pour une charge de travail PUT de 100 %, $P = 1$, et pour une charge DE travail GET de 100 %, $P = 0$).

Utilisons K pour représenter la taille moyenne de la somme des noms des comptes S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). La valeur de K est alors de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs P et K, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe doit traiter à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit par défaut (toutes les catégories définies sur Normal, sauf Storage, Qui est défini sur erreur) :

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est PUT à 50 %, et les noms de compte S3, les noms de compartiment, Et les noms d'objet utilisent une moyenne de 90 octets. Votre serveur syslog externe doit être dimensionné pour prendre en charge 1,500 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux d'environ 1 Mo par seconde.

Formules d'estimation pour les niveaux d'audit non par défaut

Les formules fournies pour les journaux d'audit supposent l'utilisation des paramètres par défaut du niveau d'audit (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur). Les formules détaillées d'estimation du taux et de la taille moyenne des messages d'audit pour les paramètres de niveau d'audit non par défaut ne sont pas disponibles. Toutefois, le tableau suivant peut être utilisé pour faire une estimation approximative du taux; vous pouvez utiliser la formule de taille moyenne fournie pour les journaux d'audit, mais sachez qu'elle risque de générer une surestimation car les messages d'audit « supplémentaires » sont, en moyenne, inférieurs aux messages d'audit par défaut.

Condition	Formule
Réplication : niveaux d'audit tous définis sur débogage ou Normal	Débit du journal d'audit = 8 x taux d'opérations S3
Codage d'effacement : les niveaux d'audit sont tous définis sur débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

Formules d'estimation pour les événements de sécurité

Les événements de sécurité ne sont pas corrélés avec les opérations S3 et produisent généralement un volume négligeable de journaux et de données. Pour ces raisons, aucune formule d'estimation n'est fournie.

Formules d'estimation pour les journaux d'application

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grid est censé prendre en charge, vous pouvez estimer le volume des journaux d'applications que votre serveur syslog externe devra gérer à l'aide des formules suivantes :

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 3,300 journaux d'application par seconde et être capable de recevoir (et de stocker) les données de journaux d'application à un taux de 1.2 Mo par seconde environ.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'applications, les variables supplémentaires les plus importantes sont la stratégie de protection des données (réplication vs code d'effacement), le pourcentage d'opérations S3 PUT (vs. Gets/autre) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs de journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Touche S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Exemples d'estimations de dimensionnement

Cette section explique des exemples d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- La réplication
- Le code d'effacement

Si vous utilisez la réplication pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, $0 \leq P \leq 1$ (pour une charge de travail PUT de 100 %, $P = 1$ et POUR une charge DE travail GET de 100 %, $P = 0$).

K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K , vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est utilisé à 50 % et les noms de comptes S3, de compartiments et de noms d'objet moyenne à 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1800 journaux d'applications par seconde. Et sera en mesure de recevoir (et de stocker en général) des données d'application à un taux de 0.5 Mo par seconde.

Si vous utilisez le code d'effacement pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, $0 \leq P \leq 1$ (pour une charge de travail PUT de 100 %, $P = 1$ et POUR une charge DE travail GET de 100 %, $P = 0$).

K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3.

Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K, vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 + (0.9 x K))) Bytes
```

Par exemple, si votre grid est dimensionné pour 1,000 opérations S3 par seconde, votre workload pèse 50 % du volume et vos noms de compte S3, noms de compartiment, les noms d'objets sont en moyenne de 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,250 journaux d'applications par seconde et être capable de recevoir (et généralement de stocker) des données d'application à un taux de 0.6 Mo par seconde.

Configurer la gestion des journaux dans StorageGRID

Configurez, selon les besoins, les niveaux d'audit, les en-têtes de protocole, l'emplacement des messages et des journaux d'audit, ainsi que la durée de conservation des journaux.

Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système. Les messages d'audit et les journaux sont des outils essentiels pour la surveillance et le débogage.

Vous pouvez, si vous le souhaitez, "[configurer un serveur syslog externe](#)" enregistrer les informations d'audit à distance. Vous pouvez minimiser l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit en utilisant un serveur 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.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".
- Si vous envisagez de configurer un serveur syslog externe, vous avez examiné et suivi les "[considérations relatives à l'utilisation d'un serveur syslog externe](#)".
- Si vous prévoyez de configurer un serveur syslog externe à l'aide du protocole TLS ou RELP/TLS, vous disposez des certificats CA serveur et client requis et de la clé privée 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 de vérification	Paramètre par défaut	Plus d'informations
Système	Normale	"Messages d'audit système"

Catégorie de vérification	Paramètre par défaut	Plus d'informations
Stockage	Erreur	"Messages d'audit du stockage objet"
Gestion	Normale	"Message d'audit de gestion"
Lectures du client	Normale	"Messages d'audit de lecture du client"
Écritures des clients	Normale	"Écrire des messages d'audit client"
ILM	Normale	"Messages d'audit ILM"
Réplication entre plusieurs grilles	Erreur	"CGRR : demande de réplication croisée"



Lors des mises à niveau, les configurations de niveau d'audit ne seront pas effectives immédiatement.

Étapes

1. Sélectionnez **Configuration > Surveillance > Gestion des journaux**.
2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Arrêt	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 » (SUCCS).
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.



Si vous n'avez pas besoin d'un enregistrement détaillé des opérations de lecture 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**.

Définissez 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.

Étapes

1. Dans la section **en-têtes de protocole d'audit**, définissez les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client.

Utilisez un astérisque (*) comme caractère générique pour qu'il corresponde à zéro ou à plusieurs caractères. Utilisez la séquence d'échappement (*) pour faire correspondre un astérisque littéral.

2. Sélectionnez **Ajouter un autre en-tête** pour créer des en-têtes supplémentaires, si nécessaire.

Lorsque StorageGRID détecte des en-têtes HTTP dans une requête, il les inclut 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**

Configurer l'emplacement du journal

Par défaut, les messages d'audit et les journaux sont enregistrés sur les nœuds où ils sont générés. StorageGRID effectue une rotation régulière et supprime finalement les messages d'audit et les journaux afin d'éviter qu'ils ne consomment un espace disque excessif. Pour enregistrer les messages d'audit et un sous-ensemble des journaux en externe, [utiliser un serveur syslog externe](#).

Si vous souhaitez enregistrer les fichiers journaux en interne, choisissez un locataire et un bucket pour le stockage des journaux et activez l'archivage des journaux.

utilisez un serveur syslog externe

Vous pouvez également 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 en dehors de votre grille.



Si vous ne souhaitez pas utiliser un serveur syslog externe, ignorez cette étape et accédez à [Sélectionnez l'emplacement du journal](#).



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 des `audit-destinations noeuds finaux`, qui se trouvent dans la section API privée de la ["API de gestion du grid"](#). 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 configurer le serveur syslog externe et fournissez les informations dont StorageGRID a besoin pour accéder au serveur syslog externe.

Étapes

1. Dans l'onglet Nœud local et serveur externe, sélectionnez **Configurer le serveur syslog externe**. Ou, si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier le serveur syslog externe**.

L'assistant configurer le serveur syslog externe s'affiche.

2. Pour l'étape **Entrez les informations syslog** de l'assistant, entrez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Host**.
3. Entrez le port de destination sur le serveur syslog externe (doit être un entier compris entre 1 et 65535). Le port par défaut est 514.
4. Sélectionnez le protocole utilisé pour envoyer les informations d'audit au serveur syslog externe.

Il est recommandé d'utiliser **TLS** ou **RELP/TLS**. Vous devez télécharger un certificat de serveur pour utiliser l'une de ces options. L'utilisation de certificats permet de sécuriser les connexions entre votre grille et le serveur syslog externe. Pour plus d'informations, voir ["Gérer les certificats de sécurité"](#).

Toutes les options de protocole requièrent la prise en charge par le serveur syslog externe ainsi que sa configuration. Vous devez choisir une option compatible avec le serveur syslog externe.



Le protocole RELP (fiable Event Logging Protocol) étend la fonctionnalité du protocole syslog afin de fournir des messages d'événement fiables. L'utilisation de RELP peut aider à éviter la perte d'informations d'audit si votre serveur syslog externe doit redémarrer.

5. Sélectionnez **Continuer**.
6. si vous avez sélectionné **TLS** ou **RELP/TLS**, téléchargez les certificats de l'autorité de certification du serveur, le certificat du 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 de clé.
 - c. Sélectionnez **Ouvrir** pour charger le fichier.

Une coche verte s'affiche en regard du nom du fichier de certificat ou de clé, vous informant qu'il a été téléchargé avec succès.

7. Sélectionnez **Continuer**.

Gérer le contenu du journal système

Vous pouvez sélectionner les informations à envoyer au serveur syslog externe.

Étapes

1. Pour l'étape **gérer le contenu syslog** de l'assistant, sélectionnez chaque type d'informations d'audit que vous souhaitez envoyer au serveur syslog externe.
 - **Envoyer les journaux d'audit** : envoie les événements StorageGRID et les activités système
 - **Envoyer des événements de sécurité** : envoie des événements de sécurité tels qu'une tentative d'ouverture de session par un utilisateur non autorisé ou une ouverture de session par un utilisateur en tant que root
 - **Envoyer les journaux d'application** : envoie des messages ["Fichiers journaux du logiciel StorageGRID"](#) utiles 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, les noeuds finaux configurés de l'équilibreur de charge et les demandes de fédération de grille à partir de systèmes distants.

2. Utilisez les menus déroulants pour sélectionner la gravité et l'établissement (type de message) pour chaque catégorie d'informations d'audit que vous souhaitez envoyer.

La définition de la gravité et des valeurs de l'établissement peut vous aider à regrouper les journaux de manière personnalisable pour une analyse plus facile.

- a. Pour **gravité**, sélectionnez **passer-système** ou sélectionnez une valeur de gravité comprise entre 0 et 7.

Si vous sélectionnez une valeur, StorageGRID l'applique à tous les messages de ce type. Vous perdez les informations relatives aux différents niveaux de gravité si vous remplacez un niveau de gravité par une valeur fixe.

Gravité	Description
Passe-système	Chaque message envoyé au syslog externe a la même valeur de gravité que lorsqu'il a été connecté localement au 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 la valeur « INFO », tandis que l'arrêt délibéré du service SSM ou RSM donne la valeur « notification ». • Pour les journaux d'accès, la gravité est « info ».
0	Urgence : le système est inutilisable
1	Alerte : une action doit être effectuée immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : conditions d'avertissement

Gravité	Description
5	Remarque : condition normale mais significative
6	Information : messages d'information
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 concernant les différents sites seront perdues si vous remplacez l'établissement par une valeur fixe.

Installation	Description
Passe-système	Chaque message envoyé au syslog externe a la même valeur d'installation que lorsqu'il a été connecté localement au nœud : • Pour les journaux d'audit, la fonction envoyée au serveur syslog externe est « local7 ». • Pour les événements de sécurité, les valeurs d'installation 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 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, la fonction envoyée au serveur syslog externe est "local0".
0	kern (messages du noyau)
1	utilisateur (messages de niveau utilisateur)
2	e-mail
3	démon (démons système)
4	auth (messages de sécurité/d'autorisation)

Installation	Description
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante ligne)
7	news (sous-système d'informations réseau)
8	UCP
9	cron (démon d'horloge)
10	sécurité (messages de sécurité/d'autorisation)
11	FTP
12	NTP
13	audit journal (audit du journal)
14	alerte journal (alerte de journal)
15	horloge (démon d'horloge)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Sélectionnez **Continuer**.

Envoyer des messages de test

Avant d'utiliser un serveur syslog externe, demandez à tous les nœuds de votre grille d'envoyer des messages de test au serveur syslog externe. Ces messages de test vous aident 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 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 les messages de test** (recommandé).

Les résultats de test apparaissent en permanence sur la page jusqu'à ce que vous arrêtez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés à vos destinations précédemment configurées.

3. Si vous recevez des erreurs lors de la configuration du serveur Syslog ou lors de l'exécution, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

Reportez-vous "[Dépanner un serveur syslog externe](#)" à pour résoudre les erreurs.

4. Attendez qu'une bannière verte indique que tous les nœuds ont réussi le test.
5. Vérifiez votre serveur syslog pour déterminer si les messages de test sont reçus et traités comme prévu.



Si vous utilisez UDP, vérifiez l'ensemble de votre infrastructure de collecte de journaux. Le protocole UDP ne permet pas une détection d'erreur aussi rigoureuse que les autres protocoles.

6. Sélectionnez **Arrêter et Terminer**.

Vous revenez à la page **Audit and syslog Server**. Une bannière verte 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.

Sélectionnez l'emplacement du journal

Vous pouvez spécifier où se trouvent les journaux d'audit, les journaux d'événements de sécurité, "[Journaux d'application StorageGRID](#)", et les journaux d'accès sont envoyés.

StorageGRID utilise par défaut les destinations d'audit de nœud local et stocke les informations d'audit dans `/var/local/log/localaudit.log`.



Lors de l'utilisation de `/var/local/log/localaudit.log`, les entrées du journal d'audit Grid Manager et tenant Manager peuvent être envoyées à un nœud de stockage. Vous pouvez trouver le nœud qui contient les entrées les plus récentes à l'aide de la `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. Sélectionnez **Emplacement du journal > Nœud local et serveur externe**.
2. Pour modifier l'emplacement du journal pour les types de journaux, sélectionnez une option différente.



Les nœuds locaux uniquement et le serveur syslog externe fournissent 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. Pour stocker les journaux pendant une période prolongée, utiliser un locataire et un bucket pour le stockage des journaux.
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 d'applications sont stockés sur les nœuds qui les ont générés. Les informations d'audit sont stockées dans les fichiers suivants : • Nœuds d'administration (primaires et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : le <code>/var/local/log/localaudit.log</code> fichier est généralement vide ou manquant. Il peut contenir des informations secondaires, telles qu'une copie supplémentaire de certains messages.

Option	Description
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 n'est activée qu'après avoir configuré un serveur syslog externe .
Nœuds 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 n'est activée qu'après avoir configuré un serveur syslog externe .

3. Sélectionnez **Enregistrer**.

Un message d'avertissement s'affiche.

4. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

Les nouveaux journaux sont envoyés aux destinations que vous avez sélectionnées. Les journaux existants restent à leur emplacement actuel.

Utiliser un seau

Les journaux sont périodiquement tournés. Utilisez un bucket S3 dans la même grille pour stocker les journaux pendant une période prolongée.

1. Sélectionnez **Emplacement du journal > Utiliser un bucket**.
2. Cochez la case **Activer les journaux d'archive**.
3. Si le locataire et le bucket répertoriés ne sont pas ceux que vous souhaitez utiliser, sélectionnez **Modifier le locataire et le bucket**, puis sélectionnez **Créer le locataire et le bucket** ou **Sélectionner le locataire et le bucket**.

Créer un locataire et un bucket

- a. Entrez un nouveau nom de locataire.
- b. Saisissez et confirmez un mot de passe pour le nouveau locataire.
- c. Entrez un nouveau nom de bucket.
- d. Sélectionnez **Créer et activer**.

Sélectionnez locataire et compartiment

- a. Sélectionnez un nom de locataire dans le menu déroulant.
- b. Sélectionnez un bucket dans le menu déroulant.
- c. Sélectionnez **Sélectionner et activer**.

4. Sélectionnez **Enregistrer**.

Les journaux seront stockés dans le locataire et le bucket que vous avez spécifiés. Le nom de la clé d'objet pour les journaux est dans ce format :

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--  
{last_modified_time}.gz
```

Par exemple :

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

Gérer la conservation des journaux

Vous pouvez gérer la durée pendant laquelle StorageGRID conserve les journaux en créant une règle ILM ou en configurant une politique de cycle de vie de compartiment S3.

Règle ILM

Créez une règle ILM pour le compartiment et ajoutez cette règle à la stratégie ILM active.

Étapes

1. Sélectionnez **ILM > règles**.
2. Sélectionnez **Créer**. "[Étape 1 \(entrer les détails\)](#)" de l'assistant Créer une règle ILM s'affiche :
 - a. Saisissez un nom unique pour la règle. Par exemple : Règle ILM pour les journaux archivés.
 - b. Sélectionnez le compte locataire S3 d'archivage des journaux.
 - c. Spécifiez le compartiment S3 d'archivage des journaux.
3. Continuez à "[Étape 2 \(définir les placements\)](#)" et définissez l'emplacement pour la règle des journaux archivés. Par exemple, la règle ILM stocke une copie répliquée sur le site 1 et une copie répliquée sur le site 2 pendant la première année. Après un an, une copie à codage d'effacement 2+1 est créée et enregistrée sur un seul site.
4. Après avoir créé la règle, ajoutez-la à une stratégie ILM active.

cycle de vie d'un compartiment S3

Configurez une stratégie de cycle de vie S3 sur le compartiment S3 d'archivage des journaux :

```
{
  "Rules": [
    {
      "ID": "Retain logs forever",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {}
    }
  ]
}
```

Lorsque vous configurez une stratégie de cycle de vie pour un compartiment S3 d'archivage des journaux, les actions d'expiration du cycle de vie prévalent sur 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 compartiment utilisent les paramètres de rétention de la stratégie ILM. Si un objet correspond à un filtre de cycle de vie du compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de rétention de la stratégie ILM ne sont pas utilisés et il est sous-entendu que les versions de l'objet sont conservées indéfiniment.

Configurer le serveur de messagerie

En tant qu'administrateur StorageGRID, vous devez configurer un serveur de messagerie pour envoyer des notifications provenant des systèmes d'alerte et de surveillance StorageGRID qui informent vous, les autres administrateurs et le support technique des événements et problèmes du système.

Les fonctionnalités de StorageGRID qui utilisent le serveur de messagerie pour les notifications incluent les

alertes, AutoSupport et la vérification multi-administrateurs (MAV). Vous pouvez utiliser le même serveur de messagerie pour toutes les notifications.

Avant de commencer

- Vous avez le "[Autorisation d'accès racine](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".

Étapes

1. Sélectionnez **Configuration > Surveillance > Serveur de messagerie**.

La page du serveur de messagerie s'affiche.

2. Sélectionnez le menu déroulant, **Afficher les fonctionnalités pouvant nécessiter un serveur de messagerie**. Si vous souhaitez consulter les détails et les informations requises pour configurer les notifications par e-mail d'une fonctionnalité, sélectionnez **Afficher**.

Vous êtes redirigé vers la page de configuration de la fonctionnalité dans le Grid Manager. La page de configuration de chaque fonctionnalité contient une notification indiquant que vous avez besoin d'un serveur de messagerie pour envoyer des notifications par e-mail.

3. Pour configurer un serveur de messagerie depuis la page Serveur de messagerie :
 - a. Saisissez l'adresse IP ou le FQDN du serveur de messagerie.
 - b. Sélectionnez le numéro de port utilisé par le serveur de messagerie. La valeur par défaut est 25.
 - c. Pour exiger une authentification, sélectionnez **Utiliser l'authentification** et saisissez le nom d'utilisateur et le mot de passe.
 - d. Pour exiger la vérification de l'identité du serveur SMTP, sélectionnez **Utiliser le protocole TLS (Transport Layer Security)**. Ensuite :
 - i. Fournissez un bundle CA.
 - ii. Si le serveur de messagerie SMTP exige que les expéditeurs fournissent des certificats clients pour l'authentification, sélectionnez **Envoyer le certificat client**. Fournissez ensuite le certificat client et la clé privée.
 - e. Pour vérifier que vos paramètres de messagerie sont corrects, envoyez un courriel de test en saisissant l'expéditeur et le destinataire. Sélectionnez **Envoyer**.

Un message de confirmation s'affiche, indiquant qu'un e-mail de test a été envoyé.

- f. Cochez les cases de tous les destinataires d'e-mail et confirmez qu'un e-mail de test a été reçu.



Si l'e-mail n'est pas reçu dans quelques minutes ou si l'alerte **échec de notification par e-mail** est déclenchée, vérifiez vos paramètres et réessayez.

- g. Connectez-vous à tout autre nœud d'administration et envoyez un e-mail de test pour vérifier la connectivité de tous les sites.



Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité. Cela contraste avec les tests de packages AutoSupport, où tous les nœuds d'administration envoient l'e-mail de test.

4. Sélectionnez **Enregistrer**.

L'envoi d'un courriel de test n'enregistre pas vos paramètres. Vous devez sélectionner **Enregistrer**.

Les paramètres de messagerie sont enregistrés.

5. Accédez aux pages de configuration des fonctionnalités qui utilisent le serveur de messagerie et complétez les paramètres de notification par e-mail.
 - **"Alertes"**. Pour les alertes, vous pouvez également ["Configurer les notifications SNMP"](#).
 - **"AutoSupport"**. Vous pouvez envoyer des packages AutoSupport par e-mail, HTTPS ou HTTP (HTTP n'est pas recommandé).
 - **"Vérification multi-administrateurs (MAV)"**.

Utiliser la surveillance SNMP

Utilisez la surveillance SNMP dans StorageGRID

Si vous souhaitez surveiller StorageGRID à l'aide du protocole SNMP (simple Network Management Protocol), vous devez configurer l'agent SNMP inclus avec StorageGRID.

- ["Configurez l'agent SNMP"](#)
- ["Mettez à jour l'agent SNMP"](#)

Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou démon, qui fournit une MIB. La MIB StorageGRID contient des définitions de tableau et de notification pour les alertes. La base MIB contient également des informations de description du système, telles que la plateforme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID supporte également un sous-ensemble d'objets MIB-II.



Vérifiez ["Accéder aux fichiers MIB"](#) si vous souhaitez télécharger les fichiers MIB sur vos nœuds grid.

Au départ, le protocole SNMP est désactivé sur tous les nœuds. Lorsque vous configurez l'agent SNMP, tous les nœuds StorageGRID reçoivent la même configuration.

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Il fournit un accès MIB en lecture seule pour les requêtes et il peut envoyer deux types de notifications événementielle à un système de gestion :

Recouvrements

Les interruptions sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple.

Les traps sont pris en charge dans les trois versions de SNMP.

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 relance maximale ait été atteinte.

Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les notifications d'interruption et d'information sont envoyées dans les cas suivants :

- Une alerte par défaut ou personnalisée est déclenchée à tout niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez ["configurer un silence"](#) pour l'alerte. Les notifications d'alerte sont envoyées par ["Nœud d'administration de l'expéditeur préféré"](#).

Chaque alerte est associée à l'un des trois types de déroutement en fonction du niveau de gravité de l'alerte : `activeMinorAlert`, `activeMajorAlert` et `activeCriticalAlert`. Pour obtenir la liste des alertes pouvant déclencher ces interruptions, reportez-vous à la ["Référence des alertes"](#).

Prise en charge de la version SNMP

Le tableau fournit un résumé détaillé des éléments pris en charge pour chaque version de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes (OBTENIR et GETNEXT)	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification par requête	Chaîne de communauté	Chaîne de communauté	Utilisateur USM (User Security Model)
Notifications (PIÈGE et INFORMATION)	Traps uniquement	Pièges et information	Pièges et information
Authentification des notifications	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Utilisateur USM pour chaque destination d'interruption

Limites

- StorageGRID supporte l'accès MIB en lecture seule. L'accès en lecture/écriture n'est pas pris en charge.
- Tous les nœuds de la grille reçoivent la même configuration.
- SNMPv3 : StorageGRID ne prend pas en charge le mode support transport (TSM).
- SNMPv3 : le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).
- SNMPv3 : le seul protocole de confidentialité pris en charge est AES.

Configurez l'agent SNMP dans StorageGRID

Vous pouvez configurer l'agent SNMP StorageGRID pour qu'il utilise un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Description de la 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 USM (User Security Model) est prise en charge.

Tous les nœuds de la grille utilisent la même configuration SNMP.

Spécifiez 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 agent SNMP s'affiche.

2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.
3. Entrez 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 en tant que sysContact. Le contact système est généralement une adresse e-mail. Cette valeur s'applique à tous les nœuds du système StorageGRID. Le contact système peut comporter un maximum de 255 caractères.
Emplacement du système	Facultatif. Emplacement du système StorageGRID, qui est renvoyé dans les messages SNMP sous le nom sysLocation. L'emplacement du système peut être toute information utile pour identifier l'emplacement de votre système StorageGRID. Par exemple, vous pouvez utiliser l'adresse d'un établissement. Cette valeur s'applique à tous les nœuds du système StorageGRID. L'emplacement du système peut comporter un maximum de 255 caractères.
Activer les notifications d'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 n'envoie pas de notifications SNMP.
Activer les interruptions d'authentification	Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des interruptions d'authentification s'il reçoit des messages de protocole authentifiés de manière incorrecte.

Entrez des chaînes de communauté

Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section chaînes de communauté.

Lorsque le système de gestion interroge la MIB StorageGRID, il envoie une chaîne de communauté. Si la chaîne de communauté correspond à l'une des valeurs spécifiées ici, l'agent SNMP envoie une réponse au système de gestion.

Étapes

1. Pour **communauté en lecture seule**, vous pouvez éventuellement entrer 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 la chaîne de communauté « public ». 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'espace.

2. Sélectionnez **Ajouter une autre chaîne de communauté** pour ajouter des chaînes supplémentaires.

Jusqu'à cinq chaînes sont autorisées.

Créer des destinations de déroutement

Utilisez l'onglet destinations d'interruption de 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. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

Étapes

1. Pour le champ **Default trap community**, vous pouvez éventuellement saisir 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 recouvrement par défaut peut comporter 32 caractères maximum et ne peut pas contenir de caractères d'espace.

2. Pour ajouter une destination d'interruption, sélectionnez **Créer**.
3. Sélectionnez la version SNMP qui sera utilisée pour cette destination d'interruption.
4. Remplissez le formulaire Créer une destination d'interruption pour la version que vous avez sélectionnée.

SNMPv1

Si vous avez sélectionné SNMPv1 comme version, renseignez 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 l'interruption.
Port	Utilisez 162, le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

SNMPv2c

Si vous avez sélectionné SNMPv2c comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
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 déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Chaîne de communauté	Utilisez la communauté d'interruptions par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruptions. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

SNMPv3

Si vous avez sélectionné SNMPv3 comme version, renseignez ces champs.

Champ	Description
Type	Indique si la destination sera utilisée pour les interruptions ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet pour recevoir l'interruption.
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 déROUTement SNMP standard, sauf si vous avez besoin d'utiliser TCP.
Utilisateur USM	Utilisateur USM qui sera utilisé pour l'authentification. • Si vous avez sélectionné Trap, seuls les utilisateurs d'USM sans ID de moteur faisant autorité sont affichés. • Si vous avez sélectionné INFORM, seuls les utilisateurs d'USM avec des ID de moteur faisant autorité sont affichés. • Si aucun utilisateur n'est affiché : i. Créez et enregistrez la destination de l'interruption. ii. Accédez à Créez des utilisateurs USM et créez l'utilisateur. iii. Revenez à l'onglet destinations des interruptions, sélectionnez la destination enregistrée dans le tableau et sélectionnez Modifier. iv. Sélectionnez l'utilisateur.

5. Sélectionnez **Créer**.

La destination de la trappe est créée et ajoutée à la table.

Créez des adresses d'agent

Vous pouvez également utiliser l'onglet adresses des agents de 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. Entrez les informations suivantes.

Champ	Description
Protocole Internet	Indique si cette adresse utilisera IPv4 ou IPv6. Par défaut, SNMP utilise IPv4.
Protocole de transport	Indique si cette adresse utilise UDP ou TCP. Par défaut, SNMP utilise UDP.
Réseau StorageGRID	Quel réseau StorageGRID l'agent écoutera ? • Réseaux Grid, Admin et client : l'agent SNMP écoute les requêtes sur les trois réseaux. • Réseau Grid • Réseau d'administration • Réseau client 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	Éventuellement, le numéro de port sur lequel l'agent SNMP doit écouter. Le port UDP par défaut d'un agent SNMP est 161, mais vous pouvez entrer n'importe quel numéro de port inutilisé. 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.

Créez des utilisateurs USM

Si vous utilisez SNMPv3, utilisez l'onglet utilisateurs USM de la section autres configurations pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.



Pour les destinations SNMPv3 *trap*, il est recommandé de créer un utilisateur USM pour chaque nœud d'administration. Si chaque nœud d'administration ne dispose pas d'un utilisateur USM, votre système de gestion peut cesser de recevoir des notifications si le nœud d'administration principal tombe en panne.



Les destinations SNMPv3 *INFORM* doivent avoir des utilisateurs avec des ID de moteur.
SNMPv3 *trap* destination 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. Entrez les informations suivantes.

Champ	Description
Nom d'utilisateur	Un nom unique pour cet utilisateur USM. Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères et ne peuvent pas contenir de caractères d'espace. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.
Accès MIB en lecture seule	Si cette option est sélectionnée, cet utilisateur doit disposer d'un accès en lecture seule à la MIB.
ID de moteur autoritaire	Si cet utilisateur sera utilisé dans une destination INFORM, l'ID de moteur faisant autorité pour cet utilisateur. Entrez 10 à 64 caractères hexadécimaux (5 à 32 octets) sans espace. 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 moteur.
Niveau de sécurité	Le niveau de sécurité de l'utilisateur USM : • AuthPriv : cet utilisateur communique avec l'authentification et la confidentialité (cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe ainsi qu'un protocole de confidentialité et un mot de passe. • AuthNoPriv : Cet utilisateur communique avec l'authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.
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.

Champ	Description
Protocole de confidentialité	Affiché uniquement si vous avez sélectionné authPriv et toujours réglé 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.

Informations associées

["Ports utilisés pour les communications externes"](#)

Mettre à jour l'agent SNMP StorageGRID

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 Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Description de la tâche

Pour plus de détails sur chaque champ de la page agent SNMP, reportez-vous à la section ["Configurez l'agent SNMP"](#). Vous devez sélectionner **Enregistrer** au bas de la page pour valider les modifications que vous apportez à chaque onglet.

Étapes

1. Sélectionnez **Configuration > Surveillance > Agent SNMP**.

La page agent SNMP s'affiche.

2. Pour désactiver l'agent SNMP sur tous les nœuds de la 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. Si vous le souhaitez, mettez à jour les informations de la section Configuration de base :

- a. Si nécessaire, mettez à jour le **contact système** et **emplacement système**.
- b. Vous pouvez également cocher ou décocher la case **Activer les notifications d'agent SNMP** pour contrôler si l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

Lorsque cette case est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.

- c. Si vous le souhaitez, cochez ou décochez 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, vous pouvez éventuellement mettre à jour ou ajouter 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 StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

Pour plus de détails sur ce que vous devez saisir, reportez-vous à "[Créer des destinations de recouvrement](#)" la section .

- Vous pouvez également mettre à jour ou supprimer la communauté de dérouterments par défaut.

Si vous supprimez la communauté d'interruptions par défaut, vous devez d'abord vous assurer que toutes les destinations d'interruptions existantes utilisent une chaîne de communauté personnalisée.

- Pour ajouter une destination d'interruption, sélectionnez **Créer**.
 - Pour modifier une destination d'interruption, sélectionnez le bouton radio et sélectionnez **Modifier**.
 - Pour supprimer une destination d'interruption, sélectionnez le bouton radio et 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 que vous devez saisir, reportez-vous à "[Créez des adresses d'agent](#)" la section .

- Pour ajouter une adresse d'agent, sélectionnez **Créer**.
 - Pour modifier une adresse d'agent, sélectionnez le bouton radio et 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 la MIB ou à recevoir des interruptions et des informations.

Pour plus de détails sur ce que vous devez saisir, reportez-vous à "[Créez des utilisateurs USM](#)" la section .

- Pour ajouter un utilisateur USM, sélectionnez **Create**.

- Pour modifier un utilisateur USM, sélectionnez le bouton radio et 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 le supprimer et en créer un nouveau.



Si vous ajoutez ou supprimez l'ID de moteur d'un utilisateur faisant autorité et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination. Sinon, 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. Sinon, 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. Lorsque vous avez mis à jour la configuration de l'agent SNMP, sélectionnez **Enregistrer**.

Accéder aux fichiers MIB de StorageGRID

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et services gérés pour les nœuds de votre grille. Vous pouvez accéder aux fichiers MIB qui définissent les objets et les notifications pour StorageGRID. Ces fichiers peuvent être utiles pour la surveillance de votre grille.

Voir "[Utiliser la surveillance SNMP](#)" pour plus d'informations sur les fichiers SNMP et MIB.

Accéder aux fichiers MIB

Procédez comme suit pour accéder aux fichiers MIB.

Étapes

1. Sélectionnez **Configuration > Surveillance > Agent SNMP**.
2. Sur la page agent SNMP, sélectionnez le fichier à télécharger :
 - **NETAPP-STORAGEGRID-MIB.txt** : définit la table d'alertes et les notifications (traps) accessibles sur tous les nœuds d'administration.
 - **ES-NETAPP-06-MIB.mib** : définit les objets et les notifications pour les appliances basées sur E-Series.
 - **MIB_1_10.zip** : définit les objets et les notifications pour les appareils dotés d'une interface BMC.



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. Obtenir l'OID de la racine de la MIB StorageGRID :

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Résultat : .1.3.6.1.4.1.789.28669 (28669 est toujours l'OID pour StorageGRID)

b. Grep pour l'OID StorageGRID dans toute l'arborescence (utilisation de `paste` pour joindre les lignes) :

```
root@user-adml:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



La `snmptranslate` commande a de nombreuses options qui sont utiles pour explorer la MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID.

Contenu du fichier MIB

Tous les objets se trouvent sous l'OID StorageGRID.

Nom de l'objet	ID objet (OID)	Description
		Le module MIB pour les entités NetApp StorageGRID.

Objets MIB

Nom de l'objet	ID objet (OID)	Type	Accéder	Module MIB	Description
ActiveAlertCount		Integer32	Lecture seule	NETAPP-STORAGEGRID-MIB	Nombre d'alertes actives dans <code>activeAlertTable</code> .
ActiveAlertTable		Séquence d'ActiveAlertEntry	Non accessible	NETAPP-STORAGEGRID-MIB	Tableau des alertes actives dans StorageGRID.
entrée d'alerte active		Séquence	Non accessible	NETAPP-STORAGEGRID-MIB	Une seule alerte StorageGRID , indexée par ID d'alerte.
ActiveAlertId		Chaîne d'octets	Lecture seule	NETAPP-STORAGEGRID-MIB	ID de l'alerte. Uniquement unique dans l'ensemble actuel d'alertes actives.
ActiveAlertName		Chaîne d'octets	Lecture seule	NETAPP-STORAGEGRID-MIB	Nom de l'alerte.
ActiveAlertInstance		Chaîne d'octets	Lecture seule	NETAPP-STORAGEGRID-MIB	Nom de l'entité qui a généré l'alerte, en général le nom du nœud.
ActiveAlertSeverity		Chaîne d'octets	Lecture seule	NETAPP-STORAGEGRID-MIB	Gravité de l'alerte.

Nom de l'objet	ID objet (OID)	Type	Accéder	Module MIB	Description
ActiveAlertStartTime		Date et heure	Lecture seule	NETAPP-STORAGEGRID-MIB	L'heure à laquelle l'alerte a été déclenchée.

Collecte de données StorageGRID supplémentaires

Surveillez les performances PUT et GET dans StorageGRID

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, afin de faciliter l'identification des modifications qui pourraient nécessiter une investigation plus poussée.

Description de la tâche

Pour surveiller les PUT et GET, vous pouvez exécuter les commandes S3 directement depuis un poste de travail ou via l'application open source S3tester. Ces méthodes vous permettent d'évaluer la performance indépendamment des facteurs externes à StorageGRID, tels que les problèmes liés à une application client ou à un réseau externe.

Lorsque vous effectuez des tests de MISE EN PLACE et D'OBTENTION d'opérations, suivez les instructions suivantes :

- Utilisez des tailles d'objet comparables aux objets que vous ingérer dans votre grid.
- Exécutez vos opérations sur des sites locaux et distants.

Les messages du "[journal d'audit](#)" indiquent le temps total nécessaire à l'exécution de certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une demande GET S3, vous pouvez vérifier la valeur de l'attribut TIME dans le message d'audit SGET. Vous pouvez également trouver l'attribut 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 répondre à une demande, ainsi que le débit global que vous pouvez atteindre. Répétez régulièrement les mêmes tests et notez les résultats afin d'identifier les tendances qui pourraient nécessiter une enquête.

- Vous pouvez "[Téléchargez S3Tester sur github](#)".

Surveillez les opérations de vérification des objets dans StorageGRID

Le système StorageGRID peut vérifier l'intégrité des données d'objet sur les nœuds de stockage en vérifiant la présence d'objets corrompus et manquants.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".

Description de la tâche

Deux "[processus de vérification](#)" fonctionnent ensemble pour garantir l'intégrité des données :

- **Vérification de l'arrière-plan** s'exécute automatiquement, en vérifiant continuellement l'exactitude des données de l'objet.

La vérification en arrière-plan vérifie automatiquement et en continu tous les nœuds de stockage pour déterminer s'il existe des copies corrompues des données d'objet répliquées et codées par effacement. Si un problème est détecté, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir des copies stockées ailleurs dans le système. La vérification en arrière-plan ne s'exécute pas sur les objets d'un pool de stockage cloud.



L'alerte **objet corrompu non identifié détecté** est déclenchée si le système détecte un objet corrompu qui ne peut pas être corrigé automatiquement.

- **La vérification de l'existence d'objet** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données d'objet.

Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet permet de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent peut avoir une incidence sur l'intégrité des données.

Vous devez consulter régulièrement les résultats des vérifications de fond et des contrôles d'existence d'objet. Recherchez immédiatement toute instance de données d'objet corrompues ou manquantes afin de déterminer la cause première.

Étapes

1. Examiner les résultats des vérifications de base :
 - a. Sélectionnez **Nœuds > Nœud de stockage > Objets**.
 - b. Vérifier les résultats de la vérification :
 - Pour vérifier la vérification des données d'objet répliqué, consultez les attributs de 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 du fragment avec code d'effacement, sélectionnez **Storage Node > ILM** et examinez les attributs de la section Vérification du code d'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 le texte d'aide.

- Examinez les résultats des travaux de vérification de l'existence d'un objet :
 - 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 100 copies d'objets manquantes ou plus et que l'alerte **Objets potentiellement 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

Examiner les messages d'audit de StorageGRID

Les messages d'audit vous permettent de mieux comprendre le fonctionnement détaillé de votre système StorageGRID. Vous pouvez utiliser les journaux d'audit pour résoudre les problèmes et évaluer les performances.

Pendant le fonctionnement normal du système, tous les services StorageGRID génèrent des messages d'audit comme suit :

- Les messages d'audit système sont liés au système d'audit lui-même, à l'état du nœud de la grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde du service.
- Les messages d'audit du stockage objet sont liés au stockage et à la gestion des objets dans StorageGRID, notamment le stockage objet et les récupérations, les transferts entre nœuds de grille et nœuds de grille, et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont consignés lorsqu'une application client S3 demande de création, de modification ou de récupération d'un objet.
- Les messages d'audit de gestion consigne les demandes des utilisateurs vers l'API de gestion.

Chaque nœud d'administration stocke les messages d'audit dans des fichiers texte. Le partage d'audit contient le fichier actif (audit.log) ainsi que les journaux d'audit compressés des jours précédents. Chaque nœud de la grille stocke également une copie des informations d'audit générées sur le nœud.

Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

StorageGRID peut envoyer les informations d'audit par défaut ou modifier la destination :

- StorageGRID sélectionne par défaut les destinations d'audit de nœud local.
- Les entrées du journal d'audit Grid Manager et tenant Manager peuvent être envoyées à un nœud de stockage.
- Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré.
- ["En savoir plus sur la configuration de la gestion des journaux"](#) .

Pour plus de détails sur le fichier journal d'audit, le format des messages d'audit, les types de messages d'audit et les outils disponibles pour analyser les messages d'audit, reportez-vous à la section ["Examiner les journaux d'audit"](#).

Collectez les fichiers journaux et les données système de StorageGRID

Vous pouvez récupérer les fichiers journaux StorageGRID et les données système, y compris les données de configuration, et les envoyer au support technique.

Avant de commencer

- Vous êtes connecté au gestionnaire de grille sur n'importe quel nœud d'administration à l'aide d'un ["navigateur web pris en charge"](#) .
- Vous avez ["autorisations d'accès spécifiques"](#) .

Description de la tâche

Utilisez 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 `.tar.gz` fichier que vous pouvez ensuite télécharger sur votre ordinateur local ou envoyer au support technique.

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 la gestion des journaux et le serveur syslog externe"](#) .

Si le nœud d'administration utilisé pour lancer la collecte des journaux est mis hors ligne pendant celle-ci, StorageGRID ne conserve pas les résultats. Vous devez redémarrer le nœud et relancer la collecte des journaux une fois le redémarrage terminé.

Étapes

1. Sélectionnez **Support > Outils > Collecte de journaux**. Un tableau de nœuds s'affiche.
2. Sélectionnez les nœuds de grille pour lesquels vous souhaitez collecter les fichiers journaux.

Vous pouvez trier par nom de nœud, site et type de nœud. Les colonnes Type de site et Type de nœud contiennent des filtres permettant de sélectionner des sites et des types de nœuds individuels.

3. Sélectionnez **Continuer**.
4. Sélectionnez la plage de dates et d'heures 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 par un nœud d'administration pour téléchargement. Si l'un ou l'autre scénario se produit, redémarrez la collecte des journaux avec un ensemble de données plus petit.

5. Sélectionnez les types de journaux que vous souhaitez collecter.

- **Journaux d'application** : journaux spécifiques à l'application que le support technique utilise le plus fréquemment pour le dépannage. Les journaux collectés sont un sous-ensemble des journaux d'application disponibles.
- **Journaux d'audit** : Journaux contenant les messages d'audit générés pendant le fonctionnement normal du système.
- **Trace réseau** : Journaux utilisés pour le débogage du réseau.
- **Base de données Prometheus** : métriques de séries chronologiques des services sur tous les nœuds.

6. Vous pouvez également utiliser la zone de texte **Notes** pour saisir des notes sur les fichiers journaux que vous collectez.

Vous pouvez utiliser ces notes pour fournir des informations de support technique sur le problème qui vous a demandé de collecter les fichiers journaux. Vos notes sont ajoutées à un fichier appelé `info.txt`, ainsi qu'à d'autres informations sur la collection de fichiers journaux. Le `info.txt` fichier est enregistré dans le package d'archivage du fichier journal.

7. Sélectionnez **Collecter les journaux**.

Vous pouvez utiliser la page de collecte des journaux pour surveiller la progression de la collecte des fichiers journaux pour chaque nœud de grille.

Si vous recevez un message d'erreur sur la taille du journal, essayez de collecter les journaux pour une période plus courte ou pour moins de nœuds.

8. Si la collecte des journaux échoue :

- Si un message « Échec de la collecte des journaux » s'affiche, vous pouvez réessayer la collecte des journaux ou terminer la session sans réessayer.
- Si un message « Échec partiel de la collecte des journaux » s'affiche, vous pouvez réessayer la collecte des journaux, terminer la session, télécharger le fichier journal partiel ou envoyer le fichier journal partiel à AutoSupport.



Vous pouvez choisir de laisser le champ « phrase secrète de provisionnement » vide pour une nouvelle tentative standard, ou vous pouvez saisir la phrase secrète pour réessayer via SSH.

9. Une fois la collecte du fichier journal terminée :

- Sélectionnez **Télécharger** pour télécharger le `.tar.gz` déposer.
- Sélectionnez **Envoyer à AutoSupport** pour envoyer le `.tar.gz` fichier au support technique.

Le `.tar.gz` le fichier contient tous les fichiers journaux de tous les nœuds de grille où la collecte des journaux a réussi. Le combiné `.tar.gz` le fichier contient une archive de fichier journal pour chaque nœud de grille.

Le sujet du package AutoSupport est `USER_TRIGGERED_SUPPORT_BUNDLE`.

10. Sélectionnez **Terminer**.



Le `.tar.gz` le fichier est supprimé lorsque vous sélectionnez **Terminer**. Assurez-vous de télécharger ou d'envoyer le fichier en premier.

Examiner les indicateurs de support StorageGRID

Lorsque vous dépannez un problème, vous pouvez consulter les graphiques et les metrics détaillés de votre système StorageGRID en collaboration avec le support technique.

Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

La page Metrics vous permet d'accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source qui permet de collecter des metrics. Grafana est un logiciel open source permettant de visualiser les metrics.



Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications. Voir la liste de ["Metrics Prometheus couramment utilisés"](#).

Étapes

1. Comme indiqué par le support technique, sélectionnez **Support > Outils > Métriques**.

Voici un exemple de la page métriques :

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools on this page are for use by technical support. Some features and menu items within these tools are intentionally non-functional.

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 interface using the link below. You must be signed in to the Grid Manager.

<https://> 

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values. Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Cloud Storage Pool Overview	Platform Services Processing
Account Service Overview	Decommission	Replicated Read Path Overview
Alertmanager	Erasure Coding - ADE	S3 - Node
Appliance Hardware Status	Erasure Coding - Overview	S3 Control
Audit Overview	Grid	S3 Overview
Bucket Cache	ILM	S3 Select
Cache Service	Identity Service Overview	Site
Cassandra Cluster Overview	Ingests	Support
Cassandra Network Overview	Node	SSD - Warranty
Cassandra Node Overview	Node (Internal Use)	Traces
Cassandra Table Cleanup	Object Chunk Leak Overview	Traffic Classification Policy
Chunk - Operations Overview	Object Serialization Mapping	Usage Processing
Chunk - Filesystem Latency Overview	OSL - AsyncIO	Virtual Memory (vmstat)
Chunk - Filesystem Latency Details	Platform Services Commits	
Cross Grid Replication	Platform Services Overview	

2. Pour consulter les valeurs actuelles des indicateurs StorageGRID et visualiser les graphiques de ces valeurs au fil du temps, sélectionnez le lien dans la section Prometheus.

L'interface Prometheus s'affiche. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les mesures StorageGRID disponibles et pour générer des graphiques sur les mesures StorageGRID au fil du temps.



Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

3. Pour accéder aux tableaux de bord préconfigurés contenant des graphiques des métriques StorageGRID au fil du temps, sélectionnez les liens dans la section Grafana.

L'interface Grafana pour le lien que vous avez sélectionné s'affiche.



Modifier la priorisation des E/S dans StorageGRID

La priorisation des entrées/sorties (E/S) vous permet de modifier les priorités relatives des opérations d'E/S sur la grille.

Par défaut, le trafic d'E/S PUT et GET du client bénéficie de la priorité la plus élevée par rapport aux activités d'arrière-plan telles que la purge des données codées par effacement (EC) et la réparation EC. En augmentant la priorité de la purge des données codées par effacement (EC) et des activités de réparation EC, ces tâches peuvent éventuellement être exécutées plus rapidement. L'efficacité des modifications de priorité des E/S est affectée par le taux de demandes des clients, les fluctuations du trafic réseau et d'autres tâches réseau en cours.

Avant de commencer

- Consultez la page de priorisation des E/S pour déterminer les options susceptibles d'avoir un impact sur votre réseau.
- Évaluez si le trafic client en cours peut gérer en toute sécurité des temps d'attente plus longs ou des délais d'attente des clients.

- Soyez prêt à surveiller l'effet du changement de priorité et à l'ajuster si nécessaire. Ces changements sont mis en œuvre rapidement, mais leurs effets peuvent prendre des heures à devenir visibles.

Étapes

1. Sélectionnez **Support > Priorisation des E/S**.
2. (Facultatif) Modifiez la priorité de purge et de réparation EC, pour les opérations en arrière-plan qui purgent les données EC, à partir de leurs valeurs par défaut.



Utilisez la priorité de purge et de réparation EC faible par défaut pour les grilles dotées de nœuds RAID.

3. Sélectionnez **Enregistrer**.
4. Surveiller le **"métrique"** pour évaluer l'effet des changements de priorisation.

Exécutez des diagnostics dans StorageGRID

Lors du dépannage d'un problème, vous pouvez vous aider avec le support technique à exécuter des diagnostics sur votre système StorageGRID et examiner les résultats.

- ["Examinez les metrics de support"](#)
- ["Metrics Prometheus couramment utilisés"](#)

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

La page Diagnostics effectue un ensemble de contrôles de diagnostic sur l'état actuel de la grille. Chaque vérification de diagnostic peut avoir l'un des trois États suivants :

-  **Normal** : Toutes les valeurs se situent dans la plage normale.
-  **Attention** : Une ou plusieurs valeurs sont hors de la plage normale.
-  **Attention** : Une ou plusieurs des valeurs sont significativement en dehors de la plage normale.

Les États de diagnostic sont indépendants des alertes en cours et peuvent ne pas indiquer de problèmes opérationnels dans la grille. Par exemple, une vérification de diagnostic peut afficher l'état de mise en garde même si aucune alerte n'a été déclenchée.

Étapes

1. Sélectionnez **Support > Outils > Diagnostics**.

La page Diagnostics s'affiche et répertorie les résultats de chaque vérification de diagnostic. Les résultats sont triés par gravité (attention, attention, puis normale). Dans chaque gravité, les résultats sont triés par ordre alphabétique.

Dans cet exemple, un diagnostic a un statut Attention et trois diagnostics ont un statut Normal.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. 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.

 
Caution Attention
0 1

Run Diagnostics

 Node uptime	▼
 Alert silences	▼
 Appliance hardware component temperatures	▼
 Cassandra automatic restarts	▼

2. Pour en savoir plus sur un diagnostic spécifique, sélectionnez cette ligne.

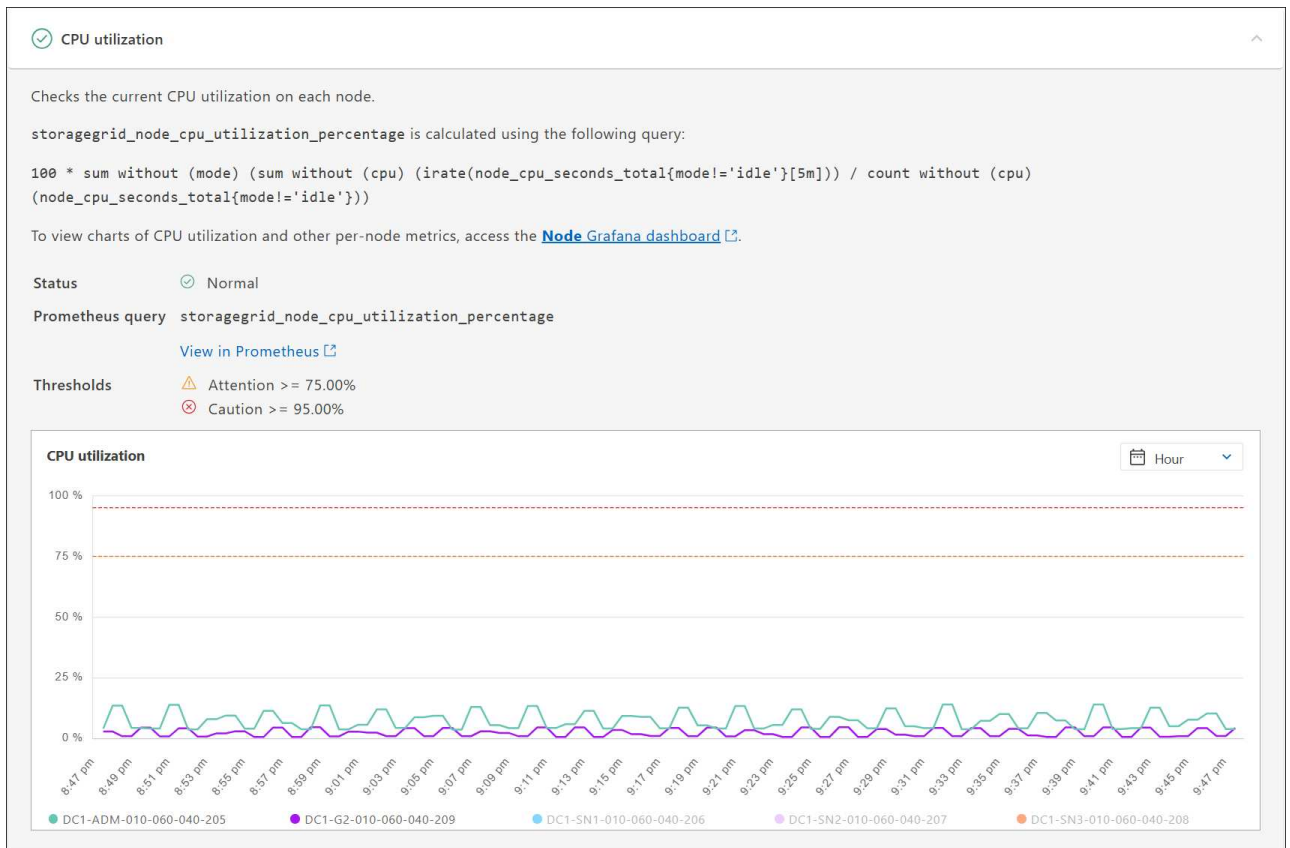
Des détails sur le diagnostic et ses résultats actuels s'affichent. Les informations suivantes sont répertoriées :

- **Etat** : état actuel de ce diagnostic : normal, attention ou attention.
- **Requête Prometheus** : si utilisé pour le diagnostic, l'expression Prometheus qui a été utilisée pour générer les valeurs d'état. (Une expression Prometheus n'est pas utilisée pour tous les diagnostics.)
- **Seuils** : si disponibles pour le diagnostic, les seuils définis par le système pour chaque état de diagnostic anormal. (Les valeurs de seuil ne sont pas utilisées pour tous les diagnostics.)



Vous ne pouvez pas modifier ces seuils.

- **Valeurs d'état** : un graphique et un tableau (tableau non affiché dans la capture d'écran) 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, sélectionnez **Tableau de bord Grafana**.

Ce lien ne s'affiche pas pour tous les diagnostics.

Le tableau de bord Grafana associé apparaît. Dans cet exemple, le tableau de bord du nœud apparaît, 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 afficher un graphique de l'expression Prometheus au fil du temps, sélectionnez **Afficher dans Prometheus**.

Un graphique Prometheus de l'expression utilisée dans le diagnostic s'affiche.

☐ 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

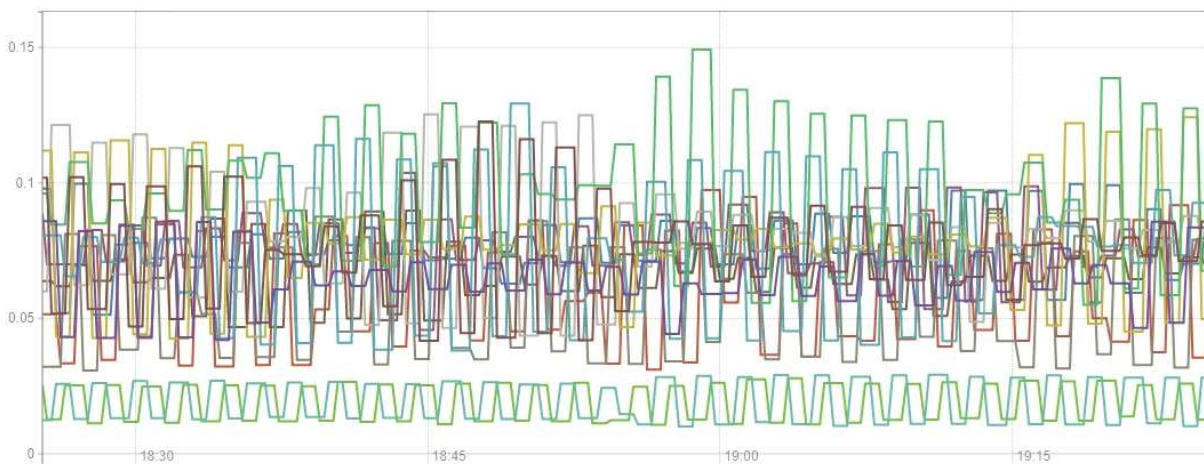
- insert metric at cursor - ▾

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

Créez des applications de surveillance personnalisées pour StorageGRID

Vous pouvez créer des applications et des tableaux de bord de surveillance personnalisés à l'aide des metrics StorageGRID disponibles dans l'API de gestion du grid.

Si vous souhaitez surveiller des mesures qui ne s'affichent pas sur une page existante du Gestionnaire de grille ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API de gestion de grille pour interroger les mesures StorageGRID.

Vous pouvez également accéder directement à des metrics Prometheus à l'aide d'un outil de surveillance externe tel que Grafana. Pour utiliser un outil externe, vous devez télécharger ou générer un certificat de client d'administration afin de permettre à StorageGRID d'authentifier l'outil pour la sécurité. Voir la ["Instructions d'administration de StorageGRID"](#).

Pour consulter les opérations de l'API des métriques, y compris la liste complète des métriques disponibles, accédez au Grid Manager. En haut de la page, sélectionnez l'icône d'aide et sélectionnez **API documentation**

> **metrics.**

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 de la mise en œuvre d’une application de surveillance personnalisée dépassent le champ d’application de cette documentation.

Dépanner le système StorageGRID

Dépanner un système StorageGRID

Si vous rencontrez un problème avec un système StorageGRID, consultez les conseils et les instructions de cette section pour déterminer et résoudre le problème.

Vous pouvez souvent résoudre vous-même certains problèmes, mais vous devrez peut-être les faire remonter au support technique.

définir le problème

La première étape pour résoudre un problème est de définir clairement le problème.

Ce tableau fournit des exemples de types d’informations que vous pouvez collecter pour définir un problème :

Question	Exemple de réponse
Que fait ou ne fait pas le système StorageGRID ? Quels sont ses symptômes ?	Les applications client signalent que les objets ne peuvent pas être ingérés dans StorageGRID.
Quand le problème a-t-il démarré ?	L’ingestion d’objet a d’abord été refusée à environ 14:50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par la demande du client. Vous avez également reçu des notifications par e-mail d’alerte.
Le problème se produit-il de manière cohérente ou seulement parfois ?	Le problème est en cours.
Si le problème se produit régulièrement, quelles sont les étapes à suivre	Un problème se produit à chaque fois qu’un client tente d’ingérer un objet.

Question	Exemple de réponse
Si le problème se produit par intermittence, quand cela se produit-il? Notez l'heure de chaque incident que vous connaissez.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème par le passé ?	C'est la première fois que j'ai vu cette question.

Évaluez les risques et l'impact sur le système

Une fois le problème défini, évaluez les risques et l'impact sur le système StorageGRID. Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services de base.

Ce tableau récapitule l'impact du problème exemple sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID est-il en mesure d'ingérer du contenu ?	Non
Les applications client peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres ne le peuvent pas.
Les données sont-elles menacées ?	Non
La capacité à mener des activités est-elle gravement affectée ?	Oui, car les applications client ne peuvent pas stocker d'objets sur le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

Collecte de données

Une fois que vous avez défini le problème et évalué ses risques et son impact, collectez des données pour analyse. Le type de données les plus utiles à recueillir dépend de la nature du problème.

Type de données à collecter	Pourquoi collecter ces données	Instructions
Créer le calendrier des modifications récentes	Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.	• Créer un calendrier des modifications récentes

Type de données à collecter	Pourquoi collecter ces données	Instructions
Consultez les alertes	Les alertes vous aident à déterminer rapidement la cause première d'un problème en fournissant des indices importants sur les problèmes sous-jacents qui pourraient l'être. Consultez la liste des alertes actuelles pour voir si StorageGRID a identifié la cause première d'un problème pour vous. Examinez les alertes déclenchées par le passé pour obtenir des informations supplémentaires.	• "Afficher les alertes actuelles et résolues"
Établir les lignes de base	Collectez des informations sur les niveaux normaux de différentes valeurs opérationnelles. Ces valeurs de référence, ainsi que les écarts par rapport à ces lignes de base, peuvent fournir des indices précieux.	• Établir les lignes de base
Tests d'entrée et de récupération	Pour résoudre les problèmes de performance liés à l'entrée et à la récupération, utilisez un poste de travail pour stocker et récupérer des objets. Comparez les résultats obtenus avec ceux observés lors de l'utilisation de l'application client.	• "Surveillez L'PUT et OBTENEZ des performances"
Examiner les messages d'audit	Examinez les messages d'audit afin de suivre les opérations StorageGRID en détail. Les détails dans les messages d'audit peuvent être utiles pour le dépannage de nombreux types de problèmes, y compris les problèmes de performance.	• "Examiner les messages d'audit"
Vérifier l'emplacement des objets et l'intégrité du stockage	En cas de problèmes de stockage, vérifiez que les objets sont placés à l'endroit où vous vous attendez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	• "Surveiller les opérations de vérification d'objets" • "Confirmer l'emplacement des données d'objet" • "Vérifiez l'intégrité de l'objet"
Collecte de données pour le support technique	L'assistance technique peut vous demander de collecter des données ou de passer en revue des informations spécifiques pour résoudre les problèmes.	• "Collecte de fichiers journaux et de données système" • "Déclencher manuellement un package AutoSupport" • "Examinez les metrics de support"

Créez un calendrier des modifications récentes

En cas de problème, vous devriez considérer ce qui a changé récemment et quand ces changements se sont produits.

- Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.
- Un calendrier des modifications peut vous aider à identifier les changements susceptibles d'être responsables d'un problème, ainsi que la manière dont chaque changement pourrait avoir affecté son développement.

Créez un tableau des dernières modifications apportées à votre système, qui contient des informations sur la date à laquelle chaque modification a eu lieu, ainsi que des informations pertinentes sur la modification, telles que les autres événements survenus pendant que la modification a été en cours :

Heure de la modification	Type de modification	Détails
Par exemple : • Quand avez-vous démarré la restauration du nœud ? • Quand la mise à niveau logicielle s'est-elle terminée ? • Avez-vous interrompu le processus ?	Que s'est-il passé ? Qu'avez-vous fait ?	Documentez toute information pertinente concernant la modification. Par exemple : • Détails des modifications du réseau. • Quel correctif a été installé. • Changement des workloads clients. Assurez-vous de noter si plusieurs changements ont eu lieu en même temps. Par exemple, ce changement a-t-il été effectué pendant qu'une mise à niveau était en cours ?

Exemples de changements récents importants

Voici quelques exemples de changements potentiellement importants :

- Le système StorageGRID a-t-il été récemment installé, étendu ou récupéré ?
- Le système a-t-il été mis à niveau récemment ? Un correctif a-t-il été appliqué ?
- Du matériel a-t-il été réparé ou modifié récemment ?
- La règle ILM a-t-elle été mise à jour ?
- La charge de travail client a-t-elle changé ?
- L'application client ou son comportement a-t-il changé ?
- Avez-vous modifié des équilibres de charge, ou ajouté ou supprimé un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Certaines tâches lancées peuvent-elles prendre un certain temps ? Voici quelques exemples :
 - Récupération d'un nœud de stockage défaillant
 - Désaffectation des nœuds de stockage
- Des modifications ont-elles été apportées à l'authentification utilisateur, par exemple l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données a-t-elle lieu ?

- Les services de plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Les pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- La compression du stockage ou le chiffrement ont-ils été modifiés ?
- L'infrastructure réseau a-t-elle été modifiée ? Par exemple, VLAN, routeurs ou DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces réseau Grid, Admin ou client ?
- Le système StorageGRID ou son environnement a-t-il subi d'autres modifications ?

Établir les lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de différentes valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base afin de détecter et de résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation de stockage moyenne	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - données d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.
Consommation moyenne des métadonnées	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - métadonnées d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.

Propriété	Valeur	Comment obtenir
Taux d'opérations S3	Opérations/seconde	Dans le tableau de bord du Grid Manager, sélectionnez Performances > Opérations S3 pour les nœuds de stockage. Pour voir les taux et les nombres d'ingestion et de récupération pour un site ou un nœud spécifique, sélectionnez Nœuds > site ou Nœud de stockage > Objets. Positionnez votre curseur sur le graphique d'ingestion et de récupération S3.
Évaluation des règles ILM	Objets/seconde	Dans la page noeuds, sélectionnez grid > ILM. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de référence du taux d'évaluation pour votre système.
Taux d'analyse ILM	Objets/seconde	Sélectionnez Nœuds > grid > ILM. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le curseur sur le graphique pour estimer la valeur de référence de Scan Rate pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez Nœuds > grid > ILM. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de base des objets mis en file d'attente (à partir des opérations client) pour votre système.
Latence moyenne des requêtes	Millisecondes	Sélectionnez Nœuds > Nœud de stockage > Objets. Dans la table Requêtes, affichez la valeur de la latence moyenne.

Analysez les données

Utilisez les informations que vous recueillez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Identifiez les points de défaillance et les goulots d'étranglement à l'aide des alertes.
- Reconstituez l'historique des problèmes à l'aide de l'historique des alertes et des graphiques.
- Utilisez les tableaux pour rechercher des anomalies et comparer la situation du problème avec le fonctionnement normal.

Liste de contrôle des informations de réaffectation

Si vous ne parvenez pas à résoudre le problème par vous-même, contactez le support technique. Avant de contacter le support technique, collectez les informations du tableau ci-dessous pour faciliter la résolution de votre problème.

	Élément	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il démarré ? Cela se produit-il de manière cohérente ou intermittente ? Si elle est intermittente, à quelle heure s'est-elle produite ? Définissez le problème
	Évaluation de l'impact	Quelle est la gravité du problème ? Quel est l'impact sur l'application client ? • Le client a-t-il déjà été connecté avec succès ? • Le client est-il en mesure d'ingérer, de récupérer et de supprimer des données ?
	ID du système StorageGRID	Sélectionnez Maintenance > Système > Licence . L'ID système StorageGRID est affiché dans le cadre de la licence actuelle.
	Version logicielle	Dans la partie supérieure du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez About pour afficher la version StorageGRID.
	Personnalisation	Résumez le mode de configuration de votre système StorageGRID. Par exemple, énumérez les éléments suivants : • La grille utilise-t-elle la compression du stockage, le chiffrement du stockage ou la conformité ? • La méthode ILM permet-elle de répliquer des objets ou de les coder en effacement ? La ILM permet-elle la redondance des sites ? Les règles ILM utilisent-elles des comportements d'ingestion équilibrés, stricts ou Double validation ?

	Élément	Remarques
	Fichiers journaux et données système	Collectez les fichiers journaux et les données système de votre système. Sélectionnez Support > Outils > Collecte de journaux. Vous pouvez collecter les journaux pour toute la grille ou pour certains nœuds. 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 installés sur un site incluent le service ADC.
	Informations de base	Collectez les informations de base relatives aux opérations d'entrée, aux opérations de récupération et à la consommation du stockage. Établir les lignes de base
	Chronologie des modifications récentes	Créez un calendrier qui résume les modifications récentes apportées au système ou à son environnement. Créer un calendrier des modifications récentes
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre vous-même le problème, assurez-vous d'enregistrer les mesures que vous avez prises et les résultats obtenus.

Résoudre les problèmes liés au stockage et aux objets

Confirmez l'emplacement des données d'objet dans StorageGRID

Selon le problème, vous pouvez vouloir "[confirmez l'emplacement de stockage des données d'objet](#)". Par exemple, vous pouvez vérifier que la règle ILM fonctionne comme prévu et que les données d'objet sont stockées à l'emplacement prévu.

Avant de commencer

- Vous devez disposer d'un identifiant d'objet, qui peut être l'un des suivants :
 - **UUID** : identifiant unique universel de l'objet. Saisissez le UUID en majuscules.
 - **CBID** : identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.
 - **S3 bucket et clé d'objet** : lorsqu'un objet est ingéré via "[Interface S3](#)", l'application client utilise une combinaison de clé de compartiment et d'objet pour stocker et identifier l'objet.

Étapes

1. Sélectionnez **ILM > Object metadata Lookup**.
2. Saisissez l'identifiant de l'objet dans le champ **Identificateur**.

Vous pouvez saisir un UUID, un CBID ou une clé de bucket/objet S3.

3. Si vous souhaitez rechercher une version spécifique de l'objet, saisissez l'ID de version (facultatif).



4. Sélectionnez **rechercher**.

Le s'"[résultats de la recherche de métadonnées d'objet](#)" affiche. Cette page répertorie les types d'informations suivants :

- Les métadonnées système, y compris l'ID d'objet (UUID), l'ID de version (facultatif), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAHS": "2",

```

Découvrez les défaillances du stockage d'objets pour les volumes de stockage dans StorageGRID

Le stockage sous-jacent d'un nœud de stockage est divisé en magasins d'objets. Les magasins d'objets sont également appelés volumes de stockage.

Vous pouvez afficher les informations du magasin d'objets pour chaque nœud de stockage. Sélectionnez **Nœuds > Nœud de stockage > Stockage**.

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

Selon la nature de la défaillance, les défaillances avec un volume de stockage peuvent être reflétées dans ["alertes de volume de stockage"](#). En cas de défaillance d'un volume de stockage, réparez le volume de stockage défectueux pour restaurer le nœud de stockage à son plein fonctionnement dès que possible. Si nécessaire, vous pouvez accéder à l'onglet **Configuration** ["Placez le nœud de stockage en lecture seule"](#) pour que le système StorageGRID puisse l'utiliser pour la récupération des données tout en vous préparant à une récupération complète du serveur.

Vérifiez l'intégrité des données d'objet dans StorageGRID

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en vérifiant la présence d'objets corrompus et manquants.

Il existe deux processus de vérification : la vérification des antécédents et la vérification de l'existence des objets (anciennement appelée vérification de premier plan). Elles travaillent ensemble pour assurer l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en continu l'exactitude des données d'objet. La vérification de l'existence d'un objet peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) d'objets.

Qu'est-ce que la vérification des antécédents ?

Le processus de vérification en arrière-plan vérifie automatiquement et en continu les nœuds de stockage pour détecter des copies corrompues de données d'objet et tente automatiquement de résoudre les problèmes qu'il trouve.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets avec code d'effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan trouve un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le nœud de stockage. Une nouvelle copie non corrompue est ensuite générée et placée pour respecter les règles ILM actives. Il se peut que la nouvelle copie ne soit pas placée sur le nœud de stockage utilisé pour la copie d'origine.



Les données d'objet corrompues sont mises en quarantaine au lieu d'être supprimées du système, de sorte qu'elles soient toujours accessibles. Pour plus d'informations sur l'accès aux données d'objet en quarantaine, contactez le support technique.

- **Objets avec code d'effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet avec code d'effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les données restantes et les fragments de parité. Si le fragment corrompu ne peut pas être reconstruit, une tentative est faite pour extraire une autre copie de l'objet. Lorsque la récupération réussit, une évaluation du ILM est effectuée pour créer une copie de remplacement de l'objet avec code d'effacement.

Le processus de vérification en arrière-plan vérifie uniquement les objets sur les nœuds de stockage. Elle ne vérifie pas les objets dans un pool de stockage cloud. Les objets doivent être âgés de plus de quatre jours pour être admissibles à la vérification des antécédents.

La vérification des antécédents s'exécute à un taux continu conçu pour ne pas interférer avec les activités ordinaires du système. Impossible d'arrêter la vérification en arrière-plan. Toutefois, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous soupçonnez un problème.

Alertes liées à la vérification des antécédents

Si le système détecte un objet corrompu qu'il ne peut pas corriger automatiquement (parce que la corruption empêche l'objet d'être identifié), l'alerte **objet corrompu non identifié détecté** est déclenchée.

Si la vérification en arrière-plan ne peut pas remplacer un objet corrompu car elle ne peut pas localiser une autre copie, l'alerte **Objets potentiellement perdus** est déclenchée.

Qu'est-ce que la vérification de l'existence d'objet ?

Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence des objets ne vérifie pas les données de l'objet lui-même (la vérification en arrière-plan le fait) ; elle permet plutôt de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent pouvait affecter l'intégrité des données.

Contrairement à la vérification de l'arrière-plan, qui se produit automatiquement, vous devez démarrer manuellement un travail de vérification de l'existence d'un objet.

Le contrôle d'existence des objets lit les métadonnées de chaque objet stocké dans StorageGRID et vérifie l'existence de copies d'objet répliquées et de fragments d'objet avec code d'effacement. Les données manquantes sont traitées comme suit :

- **Copies répliquées** : si une copie des données d'objet répliqué est manquante, StorageGRID tente automatiquement de remplacer la copie d'une autre copie stockée dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM. Elle détermine que la politique ILM actuelle n'est plus respectée pour cet objet, car une autre copie est manquante. Une nouvelle copie est générée et placée pour respecter les règles 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 sur le même nœud de stockage en utilisant les fragments restants. Si le fragment manquant ne peut pas être reconstruit (en raison de la perte d'un trop grand nombre de fragments), ILM tente de trouver une autre copie de l'objet, qu'il peut utiliser pour générer un nouveau fragment avec code d'effacement.

Exécutez la vérification de l'existence d'objet

Vous créez et exécutez un travail de vérification de l'existence d'un objet à la fois. Lorsque vous créez un travail, vous sélectionnez les nœuds de stockage et les volumes à vérifier. Vous sélectionnez également la cohérence du travail.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez vérifié que les nœuds de stockage que vous souhaitez vérifier sont en ligne. Sélectionnez **Nœuds** 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 sont **non** exécutées sur les nœuds que vous voulez vérifier :
 - Extension de la grille pour ajouter un nœud de stockage
 - Désaffectation du nœud de stockage
 - Restauration d'un volume de stockage défaillant

- Récupération d'un nœud de stockage avec un lecteur système défaillant
- Rééquilibrage EC
- Clone du nœud d'appliance

Le contrôle d'existence d'objet ne fournit pas d'informations utiles pendant que ces procédures sont en cours.

Description de la tâche

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 création d'un objet Vérification de l'existence s'affiche.
3. Sélectionnez les nœuds contenant les volumes à vérifier. Pour sélectionner tous les nœuds en ligne, cochez la case **Node name** dans l'en-tête de colonne.

Vous pouvez effectuer vos recherches par nom de nœud ou site.

Vous ne pouvez pas sélectionner de nœuds qui ne sont pas connectés à la grille.

4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs volumes pour chaque nœud de la liste. Vous pouvez rechercher des volumes à l'aide du numéro du volume de stockage ou du nom du nœud.

Pour sélectionner tous les volumes pour chaque nœud sélectionné, cochez la case **Storage volume** dans l'en-tête de colonne.

6. Sélectionnez **Continuer**.
7. Sélectionnez la cohérence du travail.

La cohérence détermine le nombre de copies des métadonnées d'objet utilisées pour la vérification de l'existence des objets.

- **Site fort** : deux copies de métadonnées sur un seul site.
- **Fort-global**: Deux copies de métadonnées à chaque site.
- **Tout** (par défaut) : les trois copies des métadonnées de chaque site.

Pour plus d'informations sur la cohérence, reportez-vous aux descriptions fournies par l'assistant.

8. Sélectionnez **Continuer**.
9. Vérifiez et vérifiez vos sélections. Vous pouvez sélectionner **Précédent** pour passer à l'étape précédente de l'assistant afin de mettre à jour vos sélections.

Un travail de vérification de l'existence d'un objet est généré et exécuté jusqu'à ce que l'un des événements suivants se produise :

- Le travail se termine.
- Vous mettez en pause ou annulez le travail. Vous pouvez reprendre un travail que vous avez

interrompu, mais vous ne pouvez pas reprendre un travail que vous avez annulé.

- Le travail se bloque. L'alerte * Vérification de l'existence de l'objet a calé* est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Le travail échoue. L'alerte **échec de la vérification de l'existence de l'objet** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Un message « Service non disponible » ou « erreur de serveur interne » s'affiche. Au bout d'une minute, actualisez la page pour continuer à surveiller le travail.



Si nécessaire, vous pouvez naviguer hors de la page de vérification de l'existence d'un objet et revenir à la page de suivi du travail.

10. Pendant l'exécution du travail, affichez l'onglet **travail actif** et notez la valeur des copies d'objet manquantes détectées.

Cette valeur représente le nombre total de copies manquantes d'objets répliqués et d'objets avec code d'effacement avec un ou plusieurs fragments manquants.

Si le nombre de copies d'objets manquantes détectées est supérieur à 100, il peut y avoir un problème avec le stockage du nœud de stockage.

11. Une fois le travail terminé, prenez les mesures supplémentaires requises :

- Si les copies d'objet manquantes détectées sont nulles, aucun problème n'a été trouvé. Aucune action n'est requise.
- Si le nombre de copies d'objets manquantes détectées est supérieur à zéro et que l'alerte **Objets potentiellement 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 potentiellement perdus** a été déclenchée, l'intégrité des données peut être affectée. Contactez le support technique.
- Vous pouvez rechercher des copies d'objets potentiellement 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 des objets potentiellement perdus](#)", bien que pour les copies d'objets, vous recherchez LLST au lieu de OLST.

12. Si vous avez sélectionné une cohérence solide ou globale pour le travail, attendez environ trois semaines avant d'exécuter à nouveau le travail sur les mêmes volumes.

Lorsque StorageGRID a eu le temps d'assurer la cohérence des métadonnées pour les nœuds et les volumes inclus dans le travail, réexécuter ce travail peut effacer les copies d'objet manquantes, ou faire vérifier d'autres copies d'objet si elles ne sont pas prises en compte.

a. Sélectionnez **Maintenance > Vérification de l'existence de l'objet > Historique des tâches**.

b. Déterminez les travaux prêts à être réexécutés :

- i. Consultez la colonne **end Time** pour déterminer les tâches qui ont été exécutées il y a plus de trois semaines.
- ii. Pour ces travaux, scannez la colonne de contrôle de cohérence pour obtenir un site fort ou fort-global.

- c. Cochez la case de chaque travail à repasser, puis sélectionnez **repassage**.
- d. Dans l'assistant Réanalyser les travaux, examinez les nœuds et volumes sélectionnés et la cohérence.
- e. Lorsque vous êtes prêt à réexécuter les travaux, sélectionnez **repassage**.

L'onglet travail actif s'affiche. Tous les travaux que vous avez sélectionnés sont réexécutés comme un travail à une cohérence de site fort. Un champ **travaux connexes** de la section Détails répertorie les ID des travaux d'origine.

Résoudre l'alerte « Taille d'objet S3 PUT trop importante » dans StorageGRID

L'alerte S3 PUT Object size too large est déclenchée si un locataire tente une opération PutObject non parties qui dépasse la taille limite S3 de 5 Gio.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Déterminez les locataires qui utilisent des objets supérieurs à 5 Gio. Vous pouvez donc les informer.

Étapes

1. Accédez à **Configuration > Surveillance > Serveur d'audit et syslog**.
2. Si les écritures client sont normales, accédez au journal d'audit :

- a. Entrée `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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 (primaires et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : le <code>/var/local/log/localaudit.log</code> fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	<code>/var/local/log/localaudit.log</code>

En fonction de vos paramètres de destination d'audit, entrez : `cd /var/local/log` ou

/var/local/audit/export/

Pour en savoir plus, consultez ["Sélectionnez l'emplacement du journal"](#) .

f. Identifiez les locataires qui utilisent des objets de plus de 5 Gio.

- i. Entrée `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9] {9}"`
- ii. Pour chaque message d'audit dans les résultats, consultez le `S3AI` champ pour déterminer l'ID de compte de locataire. Utilisez les autres champs du message pour déterminer l'adresse IP utilisée par le client, le compartiment et l'objet :

Code	Description
SAIP	Adresse IP source
S3AI	ID locataire
S3BK	Godet
S3KY	Objet
CSIZ	Taille (octets)

Exemple de résultats du journal d'audit

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"060X85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Si les écritures du client ne sont pas normales, utilisez l'ID de locataire de l'alerte pour identifier le locataire :

- a. Accédez à **Support > Outils > Collecte de journaux**. Collectez les journaux d'application pour le nœud de stockage dans l'alerte. Précisez 15 minutes avant et après l'alerte. ["Collecte de fichiers journaux et de données système"](#) .
- b. Extraire le fichier et aller à `bycast.log`:

/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log

- c. Recherchez le journal `method=PUT` et identifiez 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>
```

- Indiquez aux locataires que la taille maximale de PutObject est de 5 Gio et que vous devez utiliser des téléchargements partitionnés pour les objets supérieurs à 5 Gio.
- Ignorez l'alerte pendant une semaine si l'application a été modifiée.

Dépanner les données d'objet perdues ou manquantes

Découvrez les données d'objets perdues et manquantes dans StorageGRID

Les objets peuvent être récupérés pour plusieurs raisons, y compris les demandes de lecture provenant d'une application client, les vérifications en arrière-plan des données d'objet répliquées, les réévaluations ILM et la restauration des données d'objet lors de la restauration d'un nœud de stockage.

Le système StorageGRID utilise les informations 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 potentiellement perdus** est déclenchée, comme suit :

- Pour les copies répliquées, si une autre copie ne peut pas être récupérée, l'objet est considéré comme perdu et l'alerte est déclenchée.
- Pour les copies avec code d'effacement, si une copie ne peut pas être récupérée à partir de l'emplacement attendu, l'attribut copies corrompues détectées (ECOR) est incrémenté d'une copie avant qu'une tentative de récupération d'une copie ne soit effectuée à partir d'un autre emplacement. Si aucune autre copie n'est trouvée, l'alerte est déclenchée.

Vous devez examiner immédiatement toutes les alertes **Objets potentiellement 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 potentiellement perdus"](#) . Les alertes d'objet perdu peuvent être déclenchées à tort par mesure de précaution.

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 potentiellement perdus"](#) pour éviter que les objets perdus connus ne masquent les nouveaux objets perdus.

Résolvez l'alerte relative aux objets potentiellement perdus dans StorageGRID

Lorsque l'alerte **Objets potentiellement 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 Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

L'alerte **Objets potentiellement perdus** indique que, selon les informations disponibles dans StorageGRID, il n'existe aucune copie d'un objet dans la grille. Les données ont peut-être été définitivement perdues.

Recherchez immédiatement les alertes relatives à la perte d'objet. Vous devrez peut-être prendre des mesures pour éviter d'autres pertes de données. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous prenez une action d'invite.



Si plus de 10 objets sont signalés comme perdus, contactez le support technique. Ne suivez pas cette procédure vous-même.

Étapes

1. Sélectionnez **Nœuds**.
2. Sélectionnez **Storage Node > objets**.
3. Vérifiez le nombre d'objets perdus affichés dans le tableau nombres d'objets.

Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquant dans l'ensemble du système StorageGRID. La valeur est la somme des compteurs d'objets perdus du composant de stockage de données dans les services LDR et DDS.

4. À partir d'un nœud d'administration, ["accédez au journal d'audit"](#) pour déterminer l'identifiant unique (UUID) de l'objet qui a déclenché l'alerte **Objets potentiellement perdus** :
 - a. Connectez-vous au nœud grid :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
 - b. Accédez au répertoire dans lequel se trouvent les journaux d'audit.

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 (primaires et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : le <code>/var/local/log/localaudit.log</code> fichier est généralement vide ou manquant dans ce mode.

Option	Destination
Serveur syslog externe	/var/local/log/localaudit.log

En fonction de vos paramètres de destination d'audit, entrez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez "[Sélectionnez l'emplacement du journal](#)".

- c. Utilisez `grep` pour extraire les messages d'audit 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. Rechercher les métadonnées de l'objet perdu à l'aide de l'UUID :

- a. Sélectionnez **ILM > Object metadata Lookup**.
- b. Entrez l'UUID et sélectionnez **Rechercher**.
- c. Vérifiez les emplacements dans les métadonnées et prenez les mesures appropriées :

Les métadonnées	Conclusion
<object_identifieur> d'objet introuvable	Si l'objet n'est pas trouvé, le message « ERROR":" » est renvoyé. Si l'objet n'est pas trouvé, réinitialiser le compteur d'objets potentiellement perdus pour effacer l'alerte. L'absence d'un objet indique que l'objet a été intentionnellement supprimé.
Emplacements > 0	Si des emplacements sont répertoriés dans la sortie, l'alerte Objets potentiellement perdus peut être un faux positif. Vérifiez que les objets existent. Utilisez l'ID de nœud et le chemin du fichier indiqués dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement indiqué. Si les objets existent, réinitialiser le compteur d'objets potentiellement perdus pour effacer l'alerte.

Les métadonnées	Conclusion
Emplacements = 0	S'il n'y a aucun emplacement répertorié dans la sortie, l'objet est potentiellement manquant. Contactez le support technique. L'assistance technique pourrait vous demander de vérifier si une procédure de récupération de stockage est en cours. Consultez : • "Restaurez les données d'objet vers un volume de stockage pour l'appliance" • "Restaurez les données d'objet vers le volume de stockage sur lequel le disque système est intact" • "Restauration des données d'objet sur le volume de stockage (panne de disque système)"

6. Après avoir résolu les problèmes d'objets perdus, réinitialisez le compteur Objets potentiellement perdus pour garantir que les alertes ne sont pas de faux positifs :
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez **Nœud de stockage > Tâches**.
 - c. Dans la section Réinitialiser le compteur d'objets potentiellement perdus, sélectionnez **Réinitialiser**.

Résolvez l'alerte de faible capacité de stockage des données d'objets dans StorageGRID

L'alerte **mémoire de données d'objet faible** surveille la quantité d'espace disponible pour le stockage de données d'objet sur chaque nœud de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

L'alerte **Low Object Data Storage** est déclenchée lorsque la quantité totale de données d'objet répliquées et codées par effacement sur un nœud de stockage remplit l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vrai :

```
(storagegrid_storage_utilization_data_bytes /
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cette condition :

- `storagegrid_storage_utilization_data_bytes` Est une estimation de la taille totale des données d'objet répliquées et codées d'effacement pour un nœud de stockage.
- `storagegrid_storage_utilization_usable_space_bytes` Quantité totale d'espace de stockage objet restant pour un nœud de stockage.

Si une alerte majeure ou mineure **stockage de données d'objet bas** est déclenchée, vous devez exécuter une procédure d'extension dès que possible.

Étapes

1. Sélectionnez **Alertes > Actuel**.

La page alertes s'affiche.

2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de données d'objet bas**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.



Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.

3. Vérifiez les détails dans la boîte de dialogue et notez ce qui suit :

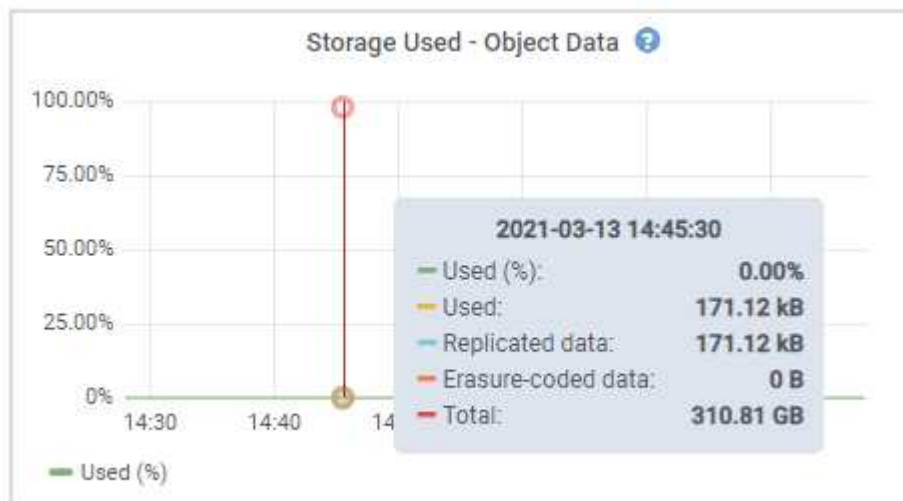
- Temps déclenché
- Le nom du site et du nœud
- Valeurs actuelles des mesures de cette alerte

4. Sélectionnez **Nœuds > Nœud de stockage ou Site > Stockage**.

5. Positionnez le curseur sur le graphique stockage utilisé - données d'objet.

Les valeurs suivantes sont affichées :

- **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
- **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
- **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code d'effacement sur ce nœud, ce site ou ce grid.
- **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` mesure.



6. Sélectionnez les commandes de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

Pour mieux comprendre la quantité de stockage utilisée auparavant et après le déclenchement de l'alerte, vous pouvez estimer le temps nécessaire pour que l'espace restant du nœud devienne complet.

7. Dès que possible, "[ajouter de la capacité de stockage](#)" à votre grille.

Vous pouvez ajouter des volumes de stockage (LUN) à des nœuds de stockage existants ou ajouter de nouveaux nœuds de stockage.



Pour plus d'informations, voir "[Gérer des nœuds de stockage complets](#)".

Résoudre l'alerte de remplacement de filigrane dans StorageGRID

Si vous utilisez des valeurs personnalisées pour les filigranes de volume de stockage, vous devrez peut-être résoudre l'alerte **dépassement de filigrane en lecture seule faible**. Si possible, vous devez mettre à jour votre système pour commencer à utiliser les valeurs optimisées.

Dans les versions précédentes, les trois "[filigranes de volume de stockage](#)" paramètres étaient globaux et la référence 8212 ; les mêmes valeurs étaient 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, des filigranes optimisés en lecture seule et en lecture-écriture sont automatiquement appliqués à tous les volumes de stockage, sauf si l'une des conditions suivantes est vraie :

- Votre système est proche de sa capacité et ne pourra pas accepter de nouvelles données si des filigranes optimisés ont été appliqués. Dans ce cas, StorageGRID ne modifie pas les paramètres du filigrane.
- Vous avez précédemment défini n'importe laquelle des filigranes du volume de stockage sur une valeur personnalisée. StorageGRID ne remplacera pas les paramètres de filigrane personnalisés avec des valeurs optimisées. Cependant, StorageGRID peut déclencher l'alerte **Low read-only filigrane override** si votre valeur personnalisée pour le filigrane soft read-only du volume de stockage est trop petite.

Description de l'alerte

Si vous utilisez des valeurs personnalisées pour les filigranes du volume de stockage, l'alerte **valeur de remplacement du filigrane en lecture seule faible** peut être déclenchée pour un ou plusieurs nœuds de stockage.

Chaque instance de l'alerte indique que la valeur personnalisée du filigrane en lecture seule souple du volume de stockage est inférieure à la valeur minimale optimisée pour ce nœud de stockage. Si vous continuez à utiliser le paramètre personnalisé, le nœud de stockage risque d'être extrêmement faible sur l'espace avant qu'il ne puisse passer en mode lecture seule en toute sécurité. Certains volumes de stockage peuvent devenir inaccessibles (lorsqu'ils sont démontés automatiquement) lorsqu'ils atteignent la capacité.

Par exemple, supposons que vous avez défini précédemment le filigrane en lecture seule souple 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 A :

Volume 0	12 GO

Volume 1	12 GO
Volume 2	11 GO
Volume 3	15 GO

L'alerte **dépassement de seuil en lecture seule faible** est déclenchée pour le nœud de stockage A car votre filigrane personnalisé (5 Go) est inférieur à la valeur minimale optimisée pour tous les volumes de ce nœud (11 Go). Si vous continuez à utiliser le paramètre personnalisé, le nœud risque d'avoir un espace insuffisant avant de passer en mode lecture seule en toute sécurité.

Résolution de l'alerte

Suivez ces étapes si une ou plusieurs alertes **prioritaire de filigrane en lecture seule basse** ont été déclenchées. Vous pouvez également utiliser ces instructions si vous utilisez actuellement des paramètres de filigrane personnalisés et souhaitez commencer à utiliser des paramètres optimisés, même si aucune alerte n'a été déclenchée.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine"](#).

Description de la tâche

Vous pouvez résoudre l'alerte **dépassement de filigrane en lecture seule** en mettant à jour les paramètres de filigrane personnalisés vers les nouveaux remplacements de filigrane. Toutefois, si un ou plusieurs nœuds de stockage sont proches de leur emplacement complet ou si vous avez des exigences ILM spécifiques, vous devez d'abord consulter les filigranes de stockage optimisés et déterminer s'il est sûr de les utiliser.

Évaluer l'utilisation des données d'objet pour l'ensemble de la grille

Étapes

1. Sélectionnez **Nœuds**.
2. Pour chaque site de la grille, développez la liste des nœuds.
3. Examinez les valeurs de pourcentage affichées dans la colonne **données objet utilisées** pour chaque nœud de stockage de chaque site.

Nodes

View the list and status of sites and grid nodes.

Search... Q 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 objet utilisées** sont inférieures à 80 %), vous pouvez commencer à utiliser les paramètres de remplacement. Allez à [Utilisez des filigranes optimisés](#).
- Si les règles ILM utilisent un comportement d'ingestion strict ou si des pools de stockage spécifiques sont proches de leur saturation, effectuez les étapes décrites dans [Afficher des filigranes de stockage optimisés](#) et [Déterminez si vous pouvez utiliser des filigranes optimisés](#).

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le seuil en lecture seule souple du volume de stockage. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

Étapes

- Sélectionnez **Support > Outils > Métriques**.
- Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
- Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Exécute** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les

volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé du filigrane en lecture seule du volume de stockage, l'alerte **Low read-only filigrane override** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

5. Notez la valeur maximale optimisée pour chaque nœud de stockage.

Déterminez si vous pouvez utiliser des filigranes optimisés

Étapes

1. Sélectionnez **Nœuds**.
2. Répétez la procédure suivante pour chaque nœud de stockage en ligne :
 - a. Sélectionnez **Storage Node > Storage**.
 - b. Faites défiler vers le bas jusqu'au tableau des magasins d'objets.
 - c. Comparez la valeur **disponible** pour chaque magasin d'objets (volume) au filigrane optimisé maximum que vous avez indiqué 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 maximum optimisé pour ce nœud, reportez-vous à la section [Utilisez des filigranes optimisés](#) pour commencer à utiliser les filigranes optimisés.

Sinon, développez la grille dès que possible. "[ajout de volumes de stockage](#)" Vers un nœud existant ou "[Ajout de nœuds de stockage](#)". Ensuite, accédez à [Utilisez des filigranes optimisés](#) pour mettre à jour les paramètres du filigrane.

4. Si vous devez continuer à utiliser des valeurs personnalisées pour les filigranes du volume de stockage "[silence](#)" ou "[désactiver](#)" l'alerte **Low read-only filigrane override**.



Les mêmes valeurs de filigrane personnalisées sont appliquées à chaque volume de stockage sur chaque nœud de stockage. L'utilisation de valeurs inférieures aux valeurs recommandées pour les filigranes du volume de stockage peut rendre certains volumes de stockage inaccessibles (démontés automatiquement) lorsque le nœud atteint sa capacité.

utiliser des filigranes optimisés

Étapes

1. Accédez à **Assistance > Autre > Filigranes de stockage**.
2. Cochez la case **utiliser les valeurs optimisées**.
3. Sélectionnez **Enregistrer**.

Les paramètres de filigrane du volume de stockage optimisé sont désormais en vigueur pour chaque volume de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

Résolvez les problèmes de métadonnées dans StorageGRID

En cas de problèmes liés aux métadonnées, 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 des métadonnées est déclenchée.

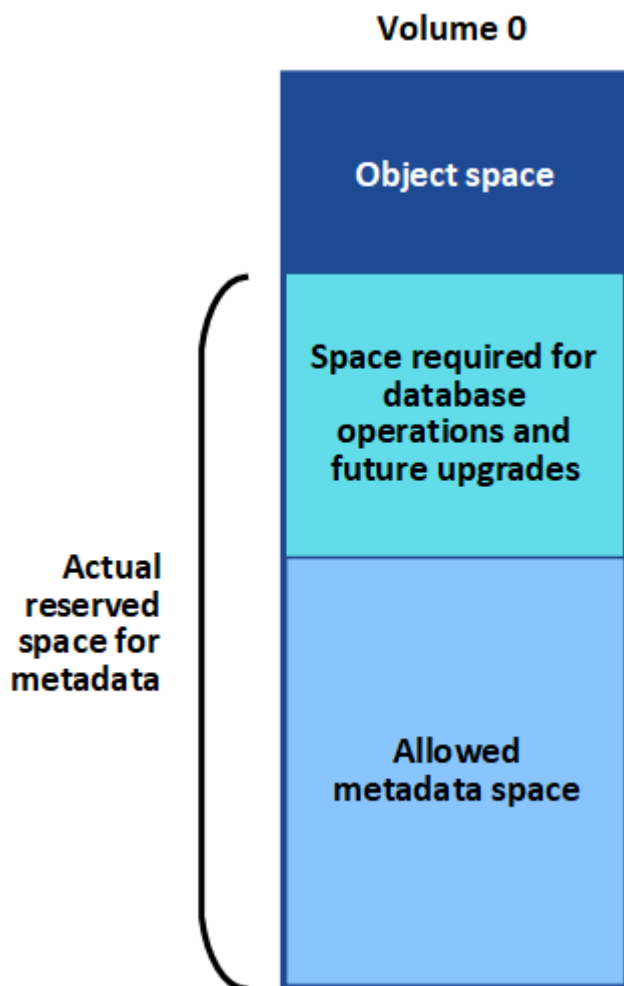
Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Suivez les actions recommandées pour chaque alerte liée aux métadonnées qui est déclenchée. Si l'alerte **stockage de métadonnées faible** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

StorageGRID réserve un certain espace sur le volume 0 de chaque nœud de stockage pour les métadonnées de l'objet. Cet espace, appelé *espace réservé réel*, est subdivisé en l'espace autorisé pour les métadonnées de l'objet (espace de métadonnées autorisé) et l'espace requis pour les opérations de base de données essentielles, telles que la compaction et la réparation. L'espace de métadonnées autorisé régit la capacité globale des objets.



Si les métadonnées d'objet consomment plus de 100 % de l'espace autorisé pour les métadonnées, les opérations de base de données ne peuvent pas s'exécuter efficacement et des erreurs se produisent.

Vous pouvez "[Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage](#)" vous aider à anticiper les erreurs et à les corriger avant qu'elles ne se produisent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer la totalité de l'espace de métadonnées autorisé :

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Lorsque cette expression Prometheus atteint certains seuils, l'alerte **stockage de métadonnées faible** est déclenchée.

- **Mineure** : les métadonnées d'objet utilisent au moins 70 % de l'espace autorisé pour les métadonnées. Vous devez ajouter des nœuds de stockage dès que possible.
- **Majeur** : les métadonnées d'objet utilisent au moins 90 % de l'espace autorisé pour les métadonnées. Vous devez immédiatement ajouter de nouveaux nœuds de stockage.



Lorsque les métadonnées d'objet utilisent au moins 90 % de l'espace de métadonnées autorisé, un avertissement s'affiche sur le tableau de bord. Si cet avertissement s'affiche, vous devez immédiatement ajouter de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées d'objet utilisent au moins 100 % de l'espace de métadonnées autorisé et commencent à consommer l'espace requis pour les opérations essentielles de la base de données. Vous devez arrêter l'ingestion des nouveaux objets et vous devez immédiatement ajouter de nouveaux nœuds de stockage.



Si la taille du volume 0 est inférieure à celle de l'option de stockage de l'espace réservé aux métadonnées (par exemple, dans un environnement non productif), le calcul de l'alerte **stockage de métadonnées faible** peut être inexact.

Étapes

1. Sélectionnez **Alertes > Actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de métadonnées faible**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Vérifiez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique **stockage de métadonnées faible** a été déclenchée, effectuez immédiatement une extension pour ajouter des nœuds de stockage.



Dans la mesure où StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité de métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du site le plus petit. Si vous devez ajouter de la capacité de métadonnées à un site, vous devez également "[développez n'importe quel autre site](#)" utiliser le même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées de l'objet existantes vers les nouveaux nœuds, qui augmentent la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **stockage de métadonnées faible** est effacée.

Dépanner les erreurs de certificat dans StorageGRID

Si vous rencontrez un problème de sécurité ou de certificat lorsque vous tentez 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.

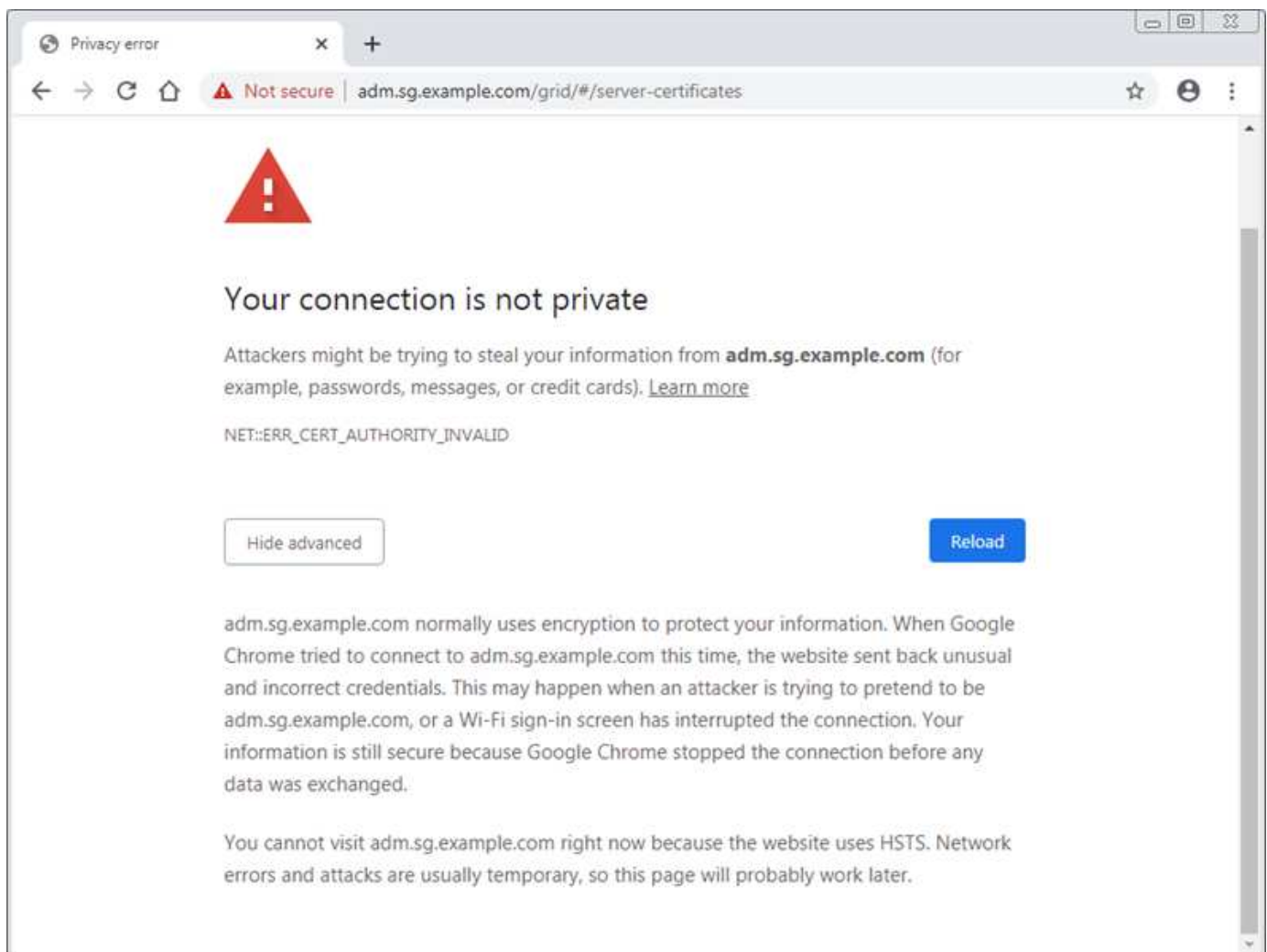
Description de la tâche

Les erreurs de certificat peuvent entraîner des problèmes lors de votre tentative de connexion à StorageGRID à l'aide de Grid Manager, de l'API de gestion du grid, du gestionnaire de locataires ou de l'API de gestion des locataires. Des erreurs de certificat peuvent également se produire lorsque vous tentez de vous connecter à un client S3 ou à un outil de surveillance externe.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez un certificat d'interface de gestion personnalisée vers le certificat de serveur par défaut.

L'exemple suivant montre une erreur de certificat lorsque le certificat de l'interface de gestion personnalisée a expiré :



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque le certificat de serveur est sur le point d'expirer.

Lorsque vous utilisez des certificats client pour l'intégration avec Prometheus externe, les erreurs de certificat peuvent être dues au certificat de l'interface de gestion StorageGRID ou aux certificats client. L'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsqu'un certificat client arrive à expiration.

Étapes

Si vous avez reçu une notification d'alerte concernant un certificat expiré, accédez aux détails du certificat : . Sélectionnez **Configuration > Sécurité > Certificats** puis ["sélectionnez l'onglet certificat approprié"](#) .

1. Vérifiez la période de validité du certificat. + certains navigateurs Web et clients S3 n'acceptent pas les certificats dont la période de validité est supérieure à 398 jours.
2. Si le certificat a expiré ou expire bientôt, téléchargez ou générez un nouveau certificat.
 - Pour un certificat de serveur, reportez-vous aux étapes de ["Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"](#).
 - Pour un certificat client, reportez-vous aux étapes de ["configuration d'un certificat client"](#).
3. Pour les erreurs de certificat de serveur, essayez l'une des options suivantes ou les deux :
 - Assurez-vous que le nom d'alternative de l'objet (SAN) du certificat est renseigné et que le SAN correspond à l'adresse IP ou au nom d'hôte du nœud auquel vous vous connectez.
 - Si vous tentez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
 - i. Entrez l'adresse IP du nœud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder à Grid Manager.
 - ii. Depuis le gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats** puis ["sélectionnez l'onglet certificat approprié"](#) pour installer un nouveau certificat personnalisé ou continuer avec le certificat par défaut.
 - iii. Dans les instructions d'administration de StorageGRID, reportez-vous aux étapes de ["Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"](#).

Résolvez les problèmes liés au nœud d'administration et à l'interface utilisateur dans StorageGRID

Vous pouvez effectuer plusieurs tâches pour 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 ou, un ["la mise en réseau"](#) problème avec ou ["matériel"](#) ["Services de nœuds d'administration"](#) ["Problème avec la base de données Cassandra"](#) sur les nœuds de stockage connectés.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le `Passwords.txt` fichier.
- Vous avez ["autorisations d'accès spécifiques"](#).

Description de la tâche

Suivez ces instructions de dépannage si vous voyez l'un des messages d'erreur suivants lorsque vous tentez de vous connecter à un 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 à nouveau de vous connecter.

Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID comporte plusieurs nœuds d'administration, essayez de vous connecter au Gestionnaire de grille à partir d'un autre nœud d'administration pour vérifier l'état d'un nœud d'administration non disponible.
 - Si vous parvenez à vous connecter, vous pouvez utiliser les options **Tableau de bord**, **Nœuds**, **Alertes** et **Assistance** pour vous aider à déterminer la cause de l'erreur.
 - Si vous n'avez qu'un seul nœud d'administration ou si vous ne pouvez toujours pas vous connecter, passez à l'étape suivante.
3. Déterminez si le matériel du nœud est hors ligne.
4. Si l'authentification unique (SSO) est activée pour votre système StorageGRID, reportez-vous à la configuration de l'authentification unique à l'aide de "[OIDC](#)" ou "[SAML](#)".

Pour résoudre ces problèmes, il peut être nécessaire de désactiver et de réactiver temporairement l'authentification SSO pour un nœud d'administration unique.

5. Déterminez si le compte que vous utilisez appartient à un utilisateur fédéré.

Si le compte d'utilisateur fédéré ne fonctionne pas, essayez de vous connecter à Grid Manager en tant qu'utilisateur local, tel que root.

- Si l'utilisateur local peut se connecter :
 - i. Consultez les alertes.
 - ii. Sélectionnez **Configuration > Contrôle d'accès > Fédération d'identité**.
 - iii. Sélectionnez **Tester la connexion** pour valider vos paramètres de connexion au serveur LDAP.
 - iv. Si le test échoue, corrigez toute erreur de configuration.
- Si l'utilisateur local ne peut pas se connecter et que vous êtes sûr que les informations d'identification sont correctes, passez à l'étape suivante.

6. Utilisez Secure Shell (SSH) pour vous connecter au nœud d'administration :
 - a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

7. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Assurez-vous que les services nms, mi, nginx et api de gestion sont tous en cours d'exécution.

La sortie est immédiatement mise à jour si l'état d'un service change.

```
$ storagegrid-status
Host Name                99-211
IP Address                10.96.99.211
Operating System Kernel  4.19.0                Verified
Operating System Environment Debian 10.1            Verified
StorageGRID Webscale Release 11.4.0                Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine          5.5.9999+default Running
Network Monitoring       11.4.0                Running
Time Synchronization     1:4.2.8p10+dfsg Running
ams                      11.4.0                Running
cmn                      11.4.0                Running
nms                      11.4.0                Running
ssm                      11.4.0                Running
mi                       11.4.0                Running
dynip                   11.4.0                Running
nginx                   1.10.3                Running
tomcat                  9.0.27                Running
grafana                  6.4.3                 Running
mgmt api                 11.4.0                Running
prometheus               11.4.0                Running
persistence              11.4.0                Running
ade exporter             11.4.0                Running
alertmanager             11.4.0                Running
attrDownPurge            11.4.0                Running
attrDownSamp1            11.4.0                Running
attrDownSamp2            11.4.0                Running
node exporter            0.17.0+ds             Running
sg snmp agent            11.4.0                Running
```

8. Vérifiez que le service nginx-gw est en cours d'exécution # `service nginx-gw status`

9. utilisez Lumberjack pour collecter les journaux : # `/usr/local/sbin/lumberjack.rb`

Si l'authentification a échoué par le passé, vous pouvez utiliser les options de script `--start` et `--end` Lumberjack pour spécifier la plage horaire appropriée. Utilisez `lumberjack -h` pour plus de détails sur ces options.

La sortie vers le terminal indique l'emplacement où l'archive de journal a été copiée.

10. consultez les journaux suivants :

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Si vous n'avez pas pu identifier de problèmes avec le nœud d'administration, exécutez l'une ou l'autre des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage exécutant le service ADC sur votre site. Il s'agit généralement des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Les nœuds Admin utilisent le service ADC pendant le processus d'authentification.

12. À partir du 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 tous les services idnt, acct, nginx et cassandra fonctionnent.

14. Répétez les étapes [Utilisez Lumberjack pour récupérer les journaux](#) et [Journaux de révision](#) pour consulter les journaux sur les nœuds de stockage.

15. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Fournissez les journaux que vous avez collectés au support technique. Voir aussi ["Référence des fichiers journaux"](#).

Problèmes liés à l'interface utilisateur

L'interface utilisateur du Gestionnaire de grille ou du Gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

Étapes

1. Assurez-vous que vous utilisez un ["navigateur web pris en charge"](#).
2. Effacez le cache de votre navigateur Web.

L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

Résolvez les problèmes de réseau, de matériel et de plateforme dans StorageGRID

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés au réseau, au matériel et à la plateforme StorageGRID.

[[422-unprocessable-entity-errors]]
== Erreurs « 422 : entité non traitable »

L'erreur 422 : entité détraitable peut se produire pour différentes raisons. Consultez le message d'erreur pour déterminer la cause de votre problème.

Si l'un des messages d'erreur répertoriés s'affiche, effectuez l'action recommandée.

Message d'erreur	Cause première et action corrective
<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 se produire si vous sélectionnez l'option ne pas utiliser TLS pour transport Layer Security (TLS) lors de la configuration de la fédération d'identités à l'aide de Windows Active Directory (AD). L'utilisation de l'option ne pas utiliser TLS n'est pas prise en charge pour les serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option Use STARTTLS ou l'option use LDAPS pour TLS.

Message d'erreur	Cause première 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) entre StorageGRID et un système externe utilisé pour identifier la fédération ou les pools de stockage dans le cloud. Vérifiez les chiffrements proposés par le système externe. Le système doit utiliser l'un des "Chiffrements pris en charge par StorageGRID" pour les connexions TLS sortantes, comme indiqué dans les instructions d'administration de StorageGRID.

alerte de non-concordance MTU du réseau de la grille

L'alerte **Grid Network MTU mismatch** est déclenchée lorsque le paramètre MTU (maximum transmission Unit) de l'interface réseau Grid (eth0) diffère considérablement sur les nœuds de la grille.

Description de la tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont configurés pour les trames jumbo. Une différence de taille de MTU supérieure à 1000 peut entraîner des problèmes de performances du réseau.

Étapes

1. L'accès SSH externe est bloqué par défaut. Si nécessaire, ["autoriser temporairement l'accès"](#) .
2. Répertorie les paramètres MTU pour eth0 sur tous les nœuds.
 - Utilisez la requête fournie dans Grid Manager.
 - Accédez à *primary Admin Node IP address/metrics/graph* et entrez la requête suivante :
`node_network_mtu_bytes{device="eth0"}`
3. ["Modifiez les paramètres MTU"](#) Si nécessaire, pour s'assurer qu'ils sont identiques pour l'interface réseau Grid (eth0) sur tous les nœuds.
 - Pour les nœuds 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 Linux, si la valeur MTU souhaitée pour le réseau dans le conteneur dépasse la valeur déjà configurée sur l'interface hôte, vous devez d'abord configurer l'interface hôte pour qu'elle ait la valeur MTU souhaitée, puis utiliser le `change-ip.py` script pour modifier la valeur MTU du réseau dans le conteneur.

Utilisez les arguments suivants pour modifier la MTU sur les nœuds Linux ou VMware.

Arguments de position	Description
mtu	La MTU à définir. Doit être compris entre 1280 et 9216.
network	Réseaux auxquels appliquer la MTU. Incluez un ou plusieurs des types de réseau suivants : • grille • admin • client

+

Arguments facultatifs	Description
-h, - help	Afficher le message d'aide et quitter.
-n node, --node node	Le nœud. La valeur par défaut est le nœud local.

4. Si vous avez autorisé l'accès SSH externe, "[bloquer l'accès](#)" lorsque vous avez terminé la tâche.

Alerte d'erreur de trame de réception réseau de nœud

Erreur de trame de réception réseau de nœud les alertes peuvent être causées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Cette alerte disparaît toute seule une fois le problème sous-jacent résolu.

Description de la tâche

Erreur de trame de réception réseau de nœud les alertes peuvent être causées par les problèmes suivants avec le matériel réseau qui se connecte à StorageGRID :

- La correction d'erreur de marche avant (FEC) est requise et n'est pas utilisée
- Le port du commutateur et la MTU de la carte réseau ne correspondent pas
- Taux d'erreur de liaison élevés
- Dépassement de la mémoire tampon de la sonnerie NIC

Étapes

1. Suivez les étapes de dépannage pour toutes les causes potentielles de cette alerte en fonction de la configuration de votre réseau.
2. Effectuez les étapes suivantes en fonction de la cause de l'erreur :

Non-concordance FEC



Ces étapes s'appliquent uniquement aux alertes **erreur de trame de réception réseau de nœud** causées par une incompatibilité FEC sur les appareils StorageGRID.

- a. Vérifiez l'état FEC du port du commutateur connecté à votre appliance StorageGRID.
- b. Vérifiez l'intégrité physique des câbles entre l'appareil et le commutateur.
- c. Si vous souhaitez modifier les paramètres FEC pour essayer de résoudre l'alerte, assurez-vous d'abord que l'appareil est configuré pour le mode **Auto** sur la page Configuration de la liaison du programme d'installation de l'appareil StorageGRID (reportez-vous aux instructions relatives à votre appareil :
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 et SG1100"
 - "SG100 et SG1000"
- d. Modifiez les paramètres FEC sur les ports du commutateur. Si possible, les ports de l'appliance StorageGRID ajustent leurs paramètres FEC.

Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID. Au lieu de cela, les appareils tentent de détecter et de mettre en miroir les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau 25 GbE ou 100 GbE, le commutateur et la carte réseau peuvent ne pas négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau revient en mode « no-FEC ». Lorsque le mode FEC n'est pas activé, les connexions sont plus susceptibles d'erreurs causées par le bruit électrique.



Les appareils StorageGRID prennent en charge les FEC Firecode (FC) et Reed Solomon (RS), ainsi qu'aucun FEC.

Le port du commutateur et la MTU de la carte réseau ne correspondent pas

Si l'alerte est causée par une incompatibilité de port de commutateur et de MTU de carte réseau, vérifiez que la taille MTU configurée sur le nœud est identique au paramètre MTU du port de commutateur.

La taille de MTU configurée sur le nœud peut être inférieure à celle définie sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à sa MTU, ce qui est possible avec cette configuration, l'alerte **erreur de trame de réception réseau de nœud** peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez la MTU du port du switch pour qu'il corresponde à la MTU de l'interface réseau StorageGRID, ou modifiez la MTU de l'interface réseau StorageGRID pour qu'elle corresponde au port du switch, en fonction de vos objectifs ou de vos exigences MTU de bout en bout.



Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Voir [Dépanner l'alerte de non-concordance de MTU du réseau Grid](#) pour plus d'informations.



Voir aussi "[Modifier le paramètre MTU](#)".

Taux d'erreur de liaison élevés

- Activez FEC, si ce n'est déjà fait.
- Vérifiez que le câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.
- Si les câbles ne semblent pas être à l'origine du problème, contactez le support technique.



Vous remarquerez peut-être des taux d'erreur élevés dans un environnement présentant un bruit électrique élevé.

Dépassement de la mémoire tampon de la sonnerie NIC

Si l'erreur est un dépassement de la mémoire tampon de la sonnerie de la carte réseau, contactez le support technique.

La mémoire tampon annulaire peut être surchargée lorsque le système StorageGRID est surchargé et ne peut pas traiter les événements réseau en temps opportun.

3. Surveillez le problème et contactez le support technique si l'alerte ne résout pas le problème.

Erreurs de synchronisation de l'heure

Des problèmes de synchronisation de l'heure peuvent s'afficher dans votre grille.

Si vous rencontrez des problèmes de synchronisation du temps, vérifiez que vous avez spécifié au moins quatre sources NTP externes, chacune fournissant une référence Stratum 3 ou supérieure, et que toutes les sources NTP externes fonctionnent normalement et sont accessibles par vos nœuds StorageGRID.



Lorsqu'"[Spécification de la source NTP externe](#)" il s'agit d'une installation StorageGRID de niveau production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

Linux : problèmes de connectivité réseau

Des problèmes de connectivité réseau peuvent survenir pour les nœuds StorageGRID hébergés sur des hôtes Linux.

Clonage d'adresses MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'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. Consultez les instructions pour "[créer des fichiers de configuration de nœud](#)".



Créez des interfaces réseau virtuelles distinctes pour le système d'exploitation hôte Linux. L'utilisation des mêmes interfaces réseau pour le système d'exploitation hôte Linux et le conteneur StorageGRID pourrait rendre le système d'exploitation hôte inaccessible.

Pour plus d'informations, consultez les instructions pour "[activer le clonage MAC](#)".

Linux : l'état du nœud est « orphelin »

Un nœud Linux à l'état orphelin indique généralement que le service StorageGRID ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est décédé de façon inattendue.

Description de la tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux à la recherche d'erreurs et de messages.
- Tentative de démarrage du nœud.
- Si nécessaire, utiliser des commandes moteur de conteneur pour arrêter le conteneur de nœuds existant.
- Redémarrez le nœud.

Étapes

1. Vérifiez les journaux du démon du service et du nœud orphelin pour voir si des erreurs évidentes et des messages relatifs à la fermeture inopinée.
2. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
3. 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 nœud StorageGRID qui contrôlent. Par exemple : `sudo docker stop --time secondscontainer-name`

Pour `seconds`, entrez le nombre de secondes que vous souhaitez attendre pour 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. Redémarrez le nœud : `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux : dépannage de la prise en charge IPv6

Vous devrez peut-être activer la prise en charge IPv6 dans le noyau si vous avez installé des nœuds StorageGRID sur des hôtes Linux et que vous remarquez que les adresses IPv6 n'ont pas été attribuées aux conteneurs de nœuds comme prévu.

Description de la tâche

Pour afficher l'adresse IPv6 qui a été attribuée à un nœud de grille :

1. Sélectionnez **Nœuds** et sélectionnez le nœud.
2. Sélectionnez **Afficher les adresses IP supplémentaires** en regard de **adresses IP** dans l'onglet vue d'ensemble.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, procédez comme suit pour activer la prise en charge IPv6 dans le noyau.

Étapes

1. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
2. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si le résultat n'est pas 0, consultez la documentation de votre système d'exploitation pour modifier les `sysctl` paramètres. Ensuite, définissez la valeur sur 0 avant de continuer.

3. Entrez le conteneur de nœuds StorageGRID : `storagegrid node enter node-name`
4. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez l'assistance technique.

5. 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 les messages d'erreur du serveur syslog externe pour StorageGRID

Le tableau suivant décrit les messages d'erreur pouvant être liés à un serveur syslog externe et répertorie les actions correctives.

Ces erreurs sont affichées par l'assistant de configuration du serveur syslog externe si vous rencontrez des problèmes lors de l'envoi de messages de test pour valider que le serveur syslog externe est correctement configuré.

Les problèmes lors de l'exécution peuvent être signalés par le ["Erreur de transfert du serveur syslog externe"](#) alerte. Si vous recevez cette alerte, suivez les instructions de l'alerte pour renvoyer les messages de test afin d'obtenir des messages d'erreur détaillés.

Pour plus d'informations sur l'envoi d'informations d'audit à un serveur syslog externe, reportez-vous à la section :

- ["Considérations relatives à l'utilisation d'un serveur syslog externe"](#)
- ["Configurer la gestion des journaux et le serveur syslog externe"](#)

Message d'erreur	Description et actions recommandées
Impossible de résoudre le nom d'hôte	Le FQDN que vous avez saisi pour le serveur syslog n'a pas pu être résolu en adresse IP. 1. Vérifiez le nom d'hôte que vous avez saisi. Si vous avez saisi une adresse IP, assurez-vous qu'elle est valide en notation W.X.Y.Z (« décimale à points »). 2. Vérifier que les serveurs DNS sont configurés correctement. 3. Vérifiez que chaque nœud peut accéder aux adresses IP du serveur DNS.
Connexion refusée	Une connexion TCP ou TLS au serveur syslog a été refusée. Il se peut qu'il n'y ait pas d'écoute de service sur le port TCP ou TLS de l'hôte, ou qu'un pare-feu bloque l'accès. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog. 2. Vérifiez que l'hôte du service syslog exécute un démon syslog écouté sur le port spécifié. 3. Vérifiez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS depuis les nœuds vers l'adresse IP et le port du serveur syslog.
Réseau inaccessible	Le serveur syslog ne se trouve pas sur un sous-réseau directement connecté. Un routeur a renvoyé un message d'échec ICMP pour indiquer qu'il n'a pas pu transférer les messages de test des nœuds répertoriés vers le serveur syslog. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Confirmez que ces éléments sont configurés pour acheminer le trafic vers le serveur syslog via l'interface réseau et la passerelle prévues (grille, Admin ou client).
Hôte inaccessible	Le serveur syslog se trouve sur un sous-réseau directement connecté (sous-réseau utilisé par les nœuds répertoriés pour leurs adresses IP Grid, Admin ou client). Les nœuds ont tenté d'envoyer des messages de test, mais n'ont pas reçu de réponses aux requêtes ARP pour l'adresse MAC du serveur syslog. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Vérifiez que l'hôte exécutant le service syslog est actif.

Message d'erreur	Description et actions recommandées
La connexion a expiré	Une tentative de connexion TCP/TLS a été effectuée, mais aucune réponse n'a été reçue depuis longtemps du serveur syslog. Il peut y avoir une mauvaise configuration de routage ou un pare-feu peut tomber du trafic sans envoyer de réponse (configuration commune). 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Vérifiez qu'ils sont configurés pour acheminer le trafic vers le serveur syslog à l'aide de l'interface réseau et de la passerelle (Grid, Admin ou client) sur lesquelles vous vous attendez à ce que le serveur syslog soit atteint. 3. Vérifiez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS à partir des nœuds répertoriés sur l'IP et le port du serveur syslog.
Connexion fermée par le partenaire	Une connexion TCP au serveur syslog a été établie avec succès, mais elle a été fermée ultérieurement. Plusieurs raisons peuvent expliquer ce phénomène : • Le serveur syslog a peut-être été redémarré ou redémarré. • Le nœud et le serveur syslog peuvent avoir des paramètres TCP/TLS différents. • Un pare-feu intermédiaire pourrait fermer les connexions TCP inactives. • Un serveur non syslog qui écoute sur le port du serveur syslog a peut-être fermé la connexion. Pour résoudre ce problème : 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog. 2. 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.
Erreur de certificat TLS	Le certificat de serveur reçu du serveur syslog n'était pas compatible avec le bundle de certificats CA et le certificat client que vous avez fournis. 1. Vérifiez que le groupe de certificats de l'autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur sur le serveur syslog. 2. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.

Message d'erreur	Description et actions recommandées
Transfert suspendu	Les enregistrements syslog ne sont plus transférés vers le serveur syslog et StorageGRID ne peut pas détecter la raison. Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale.
Session TLS interrompue	Le serveur syslog a mis fin à la session TLS et StorageGRID ne parvient pas à détecter la raison. 1. Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale. 2. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog. 3. Si vous utilisez TLS, vérifiez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP. 4. Vérifiez que le groupe de certificats de l'autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur du serveur syslog. 5. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.
Échec de la requête de résultats	Le nœud d'administration utilisé pour la configuration et le test du serveur syslog ne peut pas demander les résultats de test à partir des nœuds répertoriés. Un ou plusieurs nœuds sont peut-être en panne. 1. Suivez les étapes de dépannage standard pour vous assurer que les nœuds sont en ligne et que tous les services attendus sont en cours d'exécution. 2. Redémarrez le service ETCD sur les nœuds répertoriés.

Découvrez les problèmes de mise en cache des équilibres de charge dans StorageGRID

Découvrez les problèmes possibles liés à la mise en cache de l'équilibreur de charge et comment les résoudre.

Déterminer si une requête a été un succès dans le cache

- L'en-tête X-Cache est défini dans la réponse aux requêtes traitées par le service de cache. Codes possibles :
 - HIT: L'objet a été servi à partir du cache
 - PARTIAL-HIT: Le bucket/la clé avait un enregistrement dans le cache, mais la totalité de la plage demandée n'a pas pu être servie à partir du cache
 - STALE: Le bucket/la clé avait un enregistrement dans le cache, mais l'objet a été mis à jour depuis la dernière fois qu'il a été servi à partir du cache.
 - MISS: L'objet n'était pas dans le cache

- Le `nginx-gw/endpoint-access.log.gz` l'enregistrement de la requête inclut « `unix:/run/cache-svc/cache-svc.sock` » pour les requêtes traitées par le cache.
- Le `cache-svc/cache-svc.log` signale un message tel que « Requête 320390 : terminée avec succès (cache atteint) » ou « Requête 320375 : terminée avec succès (cache manqué) ». Recherchez le chemin demandé en recherchant d'autres enregistrements avec la même chaîne « Requête <numéro> ».

Faible taux de réussite du cache

- Des taux de réussite de cache faibles peuvent être attendus lorsqu'une nouvelle charge de travail est ajoutée ou que l'ensemble de travail auquel accède une charge de travail change. Dans ces situations, le taux de réussite devrait augmenter au fil du temps.
- Si plusieurs charges de travail utilisent la mise en cache, envisagez d'ajouter des stratégies de classification du trafic pour isoler les parties des charges de travail gérées par le cache. Les mesures du taux de réussite du cache sont disponibles selon la politique de classification du trafic. Si certaines charges de travail ne connaissent pas de bons taux de réussite du cache, envisagez de déplacer ces charges de travail vers d'autres points de terminaison sur lesquels la mise en cache n'est pas activée.
- Évaluer le taux d'éviction du cache. Si le cache est trop petit pour contenir l'ensemble de travail, il subira des taux d'expulsion élevés et pourrait contribuer à des taux de réussite inférieurs.
- Des options permettant d'améliorer les taux de réussite de certaines charges de travail peuvent être disponibles sous FPVR.

Faible performance

- Évaluer le taux de réussite du cache. Des taux de réussite du cache faibles peuvent entraîner de faibles performances globales.
- Évaluer le taux d'éviction du cache. Lors de l'expulsion, certaines ressources de stockage sont utilisées pour supprimer les objets existants du disque. Si le processus d'expulsion ne suit pas l'accès aux nouveaux objets, le système peut atteindre les seuils de filigrane dur et commencer à contourner le cache.
- Vérifiez les limites du réseau à l'aide des diagnostics « Utilisation de réception des interfaces réseau » et « Utilisation de transmission des interfaces réseau ».

Examiner les journaux d'audit

Journaux et messages d'audit

Ces instructions contiennent des informations sur la structure et le contenu des messages d'audit StorageGRID et des journaux d'audit. Vous pouvez utiliser ces informations pour lire et analyser la piste d'audit de l'activité du système.

Ces instructions s'adresse aux administrateurs responsables de la production de rapports d'activité et d'utilisation du système qui nécessitent une analyse des messages d'audit du système StorageGRID.

Pour utiliser le fichier journal texte, vous devez avoir accès au partage d'audit configuré sur le nœud d'administration.

Pour plus d'informations sur la configuration des niveaux de messages d'audit et l'utilisation d'un serveur syslog externe, consultez ["Configurer la gestion des journaux et le serveur syslog externe"](#).

Comment les messages d'audit transitent dans le système StorageGRID jusqu'au fichier `audit.log` pour conservation

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit se déplacent dans le fichier via le système StorageGRID `audit.log`.

Les flux de travail suivants pour les messages d'audit et la conservation des messages d'audit ne s'appliquent que si StorageGRID est configuré pour les **nœuds d'administration/nœuds locaux** ou **nœud d'administration et serveur syslog externe**. Si StorageGRID est configuré pour « Nœuds locaux uniquement » (par défaut) ou « Serveur syslog externe », les messages d'audit sont enregistrés localement sur chaque nœud du `/var/local/log/localaudit.log` fichier et ne peut pas être traité par les nœuds d'administration ou les nœuds de stockage.

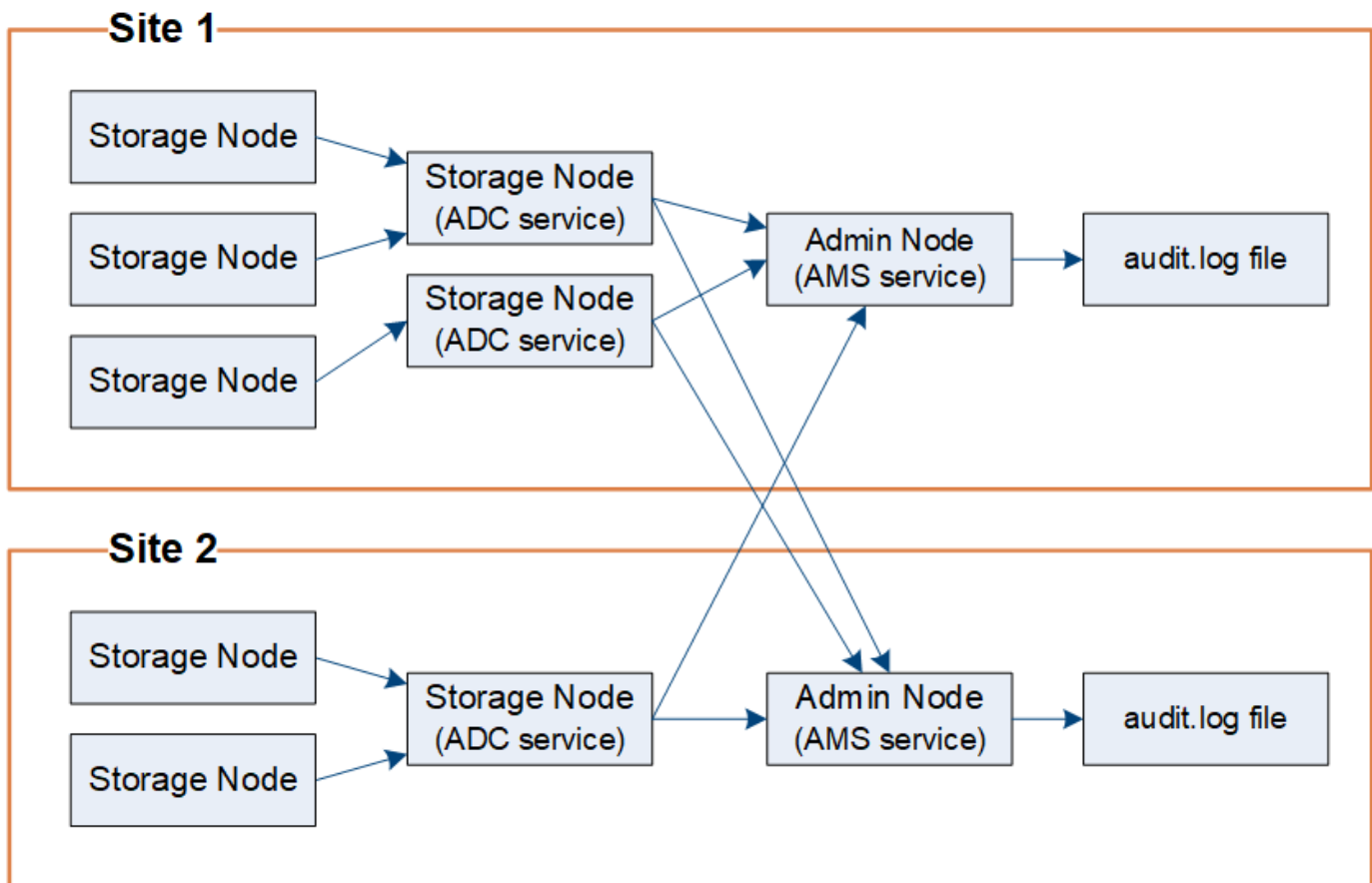
Flux de message d'audit

Les messages d'audit sont traités par les nœuds d'administration lorsque StorageGRID est configuré pour les **nœuds d'administration/nœuds locaux** ou **nœud d'administration et serveur syslog externe** et par les nœuds de stockage qui disposent d'un service de contrôleur de domaine administratif (ADC).

Comme indiqué dans le schéma de flux des messages d'audit, chaque nœud StorageGRID envoie ses messages d'audit à l'un des services ADC du site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

De son tour, chaque service ADC agit comme un relais et envoie sa collection de messages d'audit à chaque nœud d'administration du système StorageGRID, ce qui donne à chaque nœud d'administration un enregistrement complet de l'activité du système.

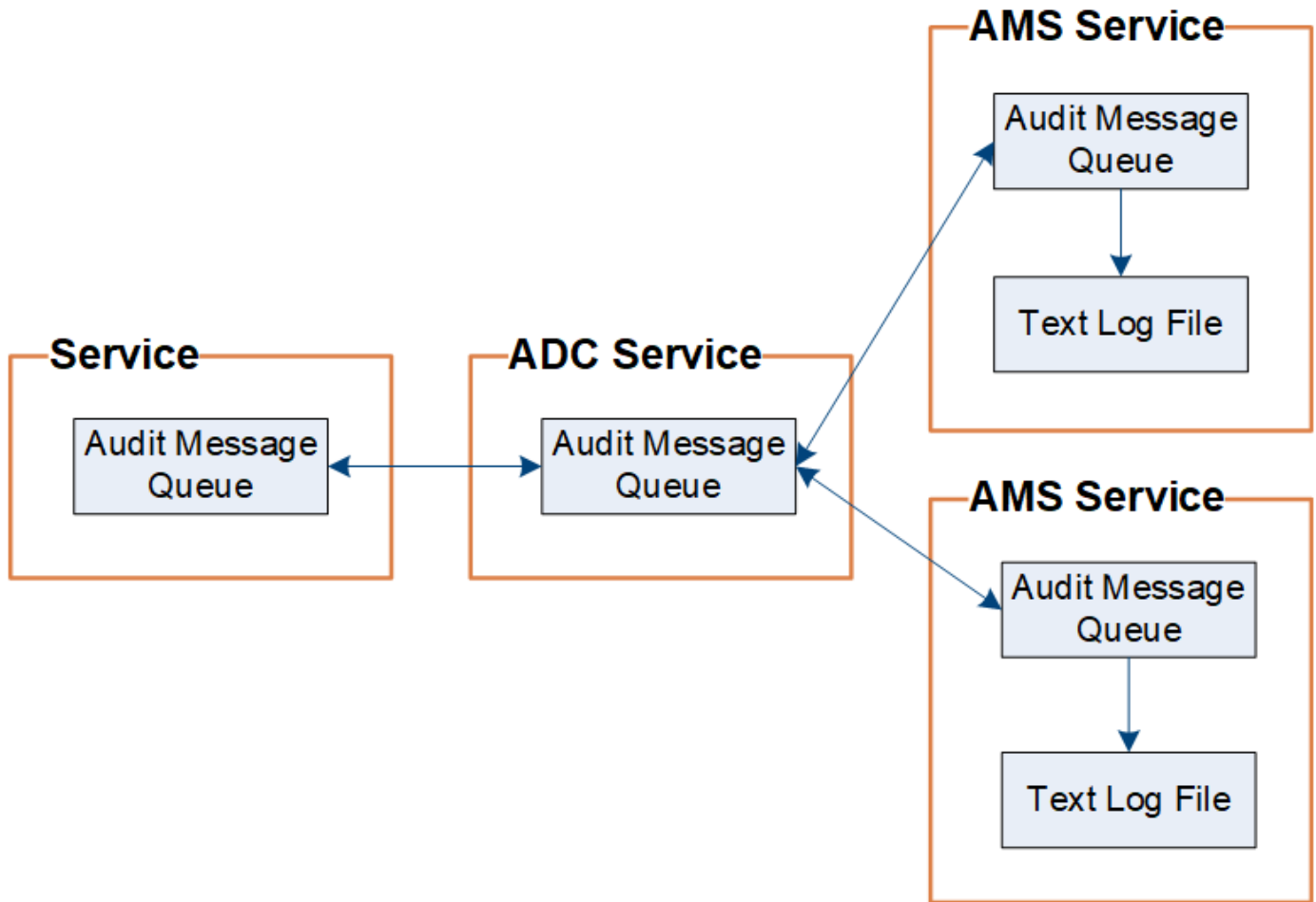
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



Conservation des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit ne soit perdu avant d'être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou 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/audit/export` 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 donnent la priorité au traitement de leur arriéré et deviennent temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pouvez voir les comportements suivants :

- Si le `/var/local/audit/export` Lorsque le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration est signalé 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/` lorsque le répertoire utilisé par un nœud de stockage avec le service ADC devient plein à 92 %, le nœud est signalé comme indisponible pour l'audit des messages 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 `/var/local/log/localaudit.log` le fichier.

- Si le `/var/local/` le répertoire utilisé par un nœud de stockage devient plein à 85 %, le nœud

commence à refuser les demandes des clients S3 avec 503 Service Unavailable .

Les types de problèmes suivants peuvent entraîner une augmentation très importante des files d'attente de messages d'audit :

- Panne d'un nœud d'administration ou d'un nœud de stockage avec le service ADC. Si l'un des nœuds du système est en panne, les nœuds restants peuvent devenir connectés à un nœud défaillant.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- L' `/var/local/` espace sur un nœud de stockage ADC devient saturé pour des raisons sans rapport avec les messages d'audit. Dans ce cas, le nœud n'accepte plus de nouveaux messages d'audit et hiérarchise son carnet de commandes actuel, ce qui peut entraîner des arriérés sur les autres nœuds.

Alerte de file d'attente d'audit et alarme de messages d'audit en file d'attente (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages d'audit dans le temps, l'alerte **grande file d'attente d'audit** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de nœud de stockage ou une file d'attente de nœud d'administration atteint certains seuils.

Si l'alerte **grande file d'attente d'audit** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge sur le système—s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme doivent être résolus au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente 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 la gestion des journaux et le serveur syslog externe](#)".

Dupliquer les messages

Le système StorageGRID adopte une approche prudente en cas de panne sur un réseau ou un nœud. Pour cette raison, des messages en double peuvent exister dans le journal d'audit.

Accédez aux fichiers du journal des audits depuis la ligne de commandes du nœud d'administration StorageGRID

Le partage d'audit contient le fichier actif `audit.log` 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.

Le `audit.log` le fichier reste vide sauf si vous configurez StorageGRID pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe**. Pour plus d'informations, reportez-vous à "[Sélectionnez l'emplacement du journal](#)".

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/audit/export/
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Découvrez la rotation des fichiers du journal des audits dans StorageGRID

Si StorageGRID est configuré pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe**, les fichiers journaux d'audit sont enregistrés sur le nœud d'administration. `/var/local/audit/export/ 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. ["Configurer les messages d'audit et le serveur syslog externe"](#).

Une fois par jour, le fichier actif `audit.log` est enregistré et un nouveau `audit.log` fichier démarre. 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 fichier utilisent la date à laquelle le fichier a été enregistré, ajoutée par un nombre, 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, le stockage du nœud d'administration alloué aux journaux d'audit est consommé. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/audit/export/ annuaire`. Les journaux d'audit sont supprimés en fonction de la date de leur création. Les journaux les plus anciens sont supprimés en premier. Vous pouvez surveiller les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre le fichier actif `audit.log`, le fichier du jour précédent (`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

Découvrez le format des fichiers journal des audits dans StorageGRID

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent un ensemble de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivi d'un espace :

YYYY-MM-DDTHH:MM:SS.UUUUUU, où *UUUUUU* sont des microsecondes.

- Le message d'audit lui-même, entre crochets et commençant par AUDT.

L'exemple suivant montre trois messages d'audit dans un fichier journal d'audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][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 le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.

Utilisez l'outil audit-explain pour traduire les messages d'audit StorageGRID

Vous pouvez utiliser `audit-explain` l'outil pour traduire les messages d'audit dans le journal d'audit dans un format facile à lire.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

L' `audit-explain` outil, disponible sur le nœud d'administration principal, fournit des résumés simplifiés des messages d'audit dans un journal d'audit.



Cet `audit-explain` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-explain` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l' `audit-explain` outil. Ces quatre "[SPUT](#)" messages d'audit ont été générés lorsque le locataire S3 associé à l'ID de compte 92484777680322627870 a utilisé des demandes PUT S3 pour créer un compartiment nommé « bucket1 » et ajouter trois objets à ce compartiment.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

L' `audit-explain` outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Comme les journaux d'audit peuvent être très volumineux et lents à analyser, vous gagnez du temps en filtrant les parties que vous souhaitez consulter et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.



`audit-explain` L'outil n'accepte pas les fichiers compressés en tant qu'entrée de tuyauterie. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l'`zcat` outil pour décompresser d'abord les fichiers. Par exemple :

```
zcat audit.log.gz | audit-explain
```

Utilisez l'`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`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

```
$ audit-explain /var/local/audit/export/audit.log
```

L'`audit-explain` outil imprime des interprétations lisibles de tous les messages du ou des fichiers spécifiés.



Pour réduire la longueur des lignes et faciliter la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l'`-t` option horodatage).

Utilisez l'outil `audit-sum` pour résumer les messages d'audit de StorageGRID

Vous pouvez utiliser `audit-sum` l'outil pour compter les messages d'audit d'écriture, de lecture, de tête et de suppression et pour afficher le temps minimal, maximal et moyen (ou la taille) pour chaque type d'opération.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Description de la tâche

L'`audit-sum` outil, disponible sur le nœud d'administration principal, récapitule le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.



Cet `audit-sum` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-sum` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

```

message group          count      min(sec)      max(sec)
average(sec)
=====
=====
IDEL                  274
SDEL                 213371        0.004        20.934
0.352
SGET                 201906        0.010       1740.290
1.132
SHEA                  22716        0.005         2.349
0.272
SPUT                 1771398        0.011       1770.563
0.487

```

Le `audit-sum` L'outil fournit les décomptes et les heures des messages d'audit S3 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 StorageGRID . Par exemple : ["StorageGRID 11.8 Utilisation de l'outil de somme d'audit"](#) .

Code	Description	Reportez-vous à la section
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	"SDEL : SUPPRESSION S3"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : TÊTE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"

L' `audit-sum` outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'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 les options de ligne de commande pour résumer les opérations sur des compartiments séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimal, maximal et moyen, mais vous pouvez utiliser l' `size (-s)` option pour examiner la taille de l'objet à la place.

Utilisez l' `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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :

- a. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

```
$ audit-sum /var/local/audit/export/audit.log
```

Cet exemple montre les résultats typiques de l'`audit-sum`outil. Cet exemple montre la durée des opérations de protocoles.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

Dans cet exemple, les opérations SGET (S3 GET) sont les opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

- b. Pour afficher les opérations de récupération 10 les plus lentes, utilisez la commande `grep` pour sélectionner uniquement les messages SGET et ajouter l'option de sortie longue (`-l`) pour inclure les chemins d'objet :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les autres messages relatifs à ces objets particuliers.

```

Total:          201906 operations
Slowest:        1740.290 sec
Average:         1.132 sec
Fastest:         0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
      1740289662      10.96.101.125      object      5663711385
backup/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-1566861764-4518.iso
      70839      10.96.101.125      object           28338
bucket3/dat.1566861764-6619
      68487      10.96.101.125      object           27890
bucket3/dat.1566861764-6615
      67798      10.96.101.125      object           27671
bucket5/dat.1566861764-6617
      67027      10.96.101.125      object           27230
bucket5/dat.1566861764-4517
      60922      10.96.101.125      object           26118
bucket3/dat.1566861764-4520
      35588      10.96.101.125      object           11311
bucket3/dat.1566861764-6616
      23897      10.96.101.125      object           10692
bucket3/dat.1566861764-4516

```

+

Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Si vous voulez déterminer la taille des objets qui sont ingérés et récupérés à partir de votre grille, utilisez l'option `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 des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :
 - a. Exécutez la commande dans le journal d'audit approprié et utilisez l'option Group-by-time (`-gt`(groupe par heure), suivie 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 tous deux considérablement plus élevés au cours de cette période, et ils n'ont pas augmenté progressivement à mesure que le nombre augmentait. Ces mesures suggèrent que la capacité a été dépassée, 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 d'hier, ajoutez l'option size (-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 des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

- c. Pour plus de détails, utilisez le ["outil d'audit-explication"](#) pour revoir toutes les opérations SGET pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande `grep` doit être de plusieurs lignes, ajoutez la `less` commande pour afficher le contenu du fichier journal d'audit, une page (un écran) à la fois.

5. Si vous souhaitez déterminer si les opérations SPUT sur les godets sont plus lentes que les opérations SPUT pour les objets :

- a. Commencez par utiliser l' ``-go`` option, qui regroupe les messages pour les opérations d'objet et de compartiment séparément :

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket	1	0.125	0.125
0.125			
SPUT.object	12	0.025	1.019
0.236			

Les résultats montrent que les opérations SPUT pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

- b. Pour déterminer les compartiments ayant les opérations SPUT les plus lentes, utilisez l'option `-gb``, qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning	71943	0.046	1770.563
1.571			
SPUT.cho-versioning	54277	0.047	1736.633
1.415			
SPUT.cho-west-region	80615	0.040	55.557
1.329			
SPUT.ldt002	1564563	0.011	51.569
0.361			

- c. Pour déterminer quels compartiments ont la taille d'objet SPUT la plus élevée, utilisez les options `-gb` et `-s` :

```
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

Découvrez la structure des messages d'audit StorageGRID

Les messages d'audit échangés dans le système StorageGRID incluent des informations standard communes à tous les messages et du contenu spécifique décrivant l'événement ou l'activité signalé.

Si les informations récapitulatives fournies par les ["audit - expliquer"](#) outils et ["somme-audit"](#) sont insuffisantes, 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 peut apparaître dans le fichier journal d'audit :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(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 entre parenthèses ([]) et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

- Entre 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 inclut un code d'attribut, un type de données et une valeur qui sont rapportées dans ce format :

```
[ATTR (type) :value] [ATTR (type) :value] ...  
[ATTR (type) :value] \n
```

Le nombre d'éléments d'attribut dans le message dépend du type d'événement du message. Les éléments d'attribut ne sont pas répertoriés dans un ordre particulier.

La liste suivante décrit les éléments d'attribut :

- **ATTR** est un code à quatre caractères pour l'attribut signalé. Certains attributs sont communs à tous les messages d'audit et à d'autres, qui sont spécifiques à un événement.
- **type** Est un identificateur à quatre caractères du type de données de programmation de la valeur, comme UI64, FC32, etc. Le type est entre parenthèses ().
- **value** est le contenu de l'attribut, généralement une valeur numérique ou textuelle. Les valeurs suivent toujours deux points (:). Les valeurs du type de données CSTR sont entourées de guillemets doubles " ".

Types de données dans les messages d'audit de StorageGRID

Différents types de données sont utilisés pour stocker les informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres 0 à 4,294,967,295.
UI64	Entier double non signé (64 bits) ; il peut stocker les nombres 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
IPAD	Utilisé pour les adresses IP.
REST	Tableau de caractères UTF-8 de longueur variable. Les caractères peuvent être échappé avec les conventions suivantes : • La barre oblique inverse est \. • Le retour chariot est \r. • Les guillemets sont \". • La ligne d'alimentation (nouvelle ligne) est \n. • Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format \XHH, où HH est la valeur hexadécimale représentant le caractère).

Données spécifiques à l'événement dans les messages d'audit StorageGRID

Chaque message d'audit du journal d'audit enregistre les données spécifiques à un événement système.

Après le conteneur d'ouverture [AUDT : 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\):"60025
621595611246499"\]
\[SACC\ (CSTR\):"account"\]\[S3AK\ (CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\ (CSTR\):"urn:sgws:identity:60025621595611246499:root"\]
\[SBAI\ (CSTR\):"60025621595611246499"\]\[SBAC\ (CSTR\):"account"\]\[S3BK\ (C
STR\):"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] [A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261\]
```

L'`ATYP`élément (souligné dans l'exemple) identifie l'événement qui a généré le message. Cet exemple de message inclut le "SHEA"code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

Éléments communs dans les messages d'audit StorageGRID

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU	FC32	ID de module : identificateur à quatre caractères de l'ID de module qui a généré le message. Ceci indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : ID de nœud de la grille attribué au service qui a généré le message. Un identifiant unique est attribué à chaque service au moment de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.
ASE	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indique l'heure à laquelle le système d'audit a été initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Remarque : cet élément est obsolète et n'apparaît plus dans les messages d'audit.

Code	Type	Description
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur a été incrémenté pour chaque message d'audit généré sur le nœud de la grille (ANID) et remis à zéro au redémarrage du service. Remarque : cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	Trace ID : identifiant partagé par l'ensemble de messages déclenchés par un seul événement.
ATIM	UI64	Timestamp: Heure à laquelle l'événement a été généré le message d'audit, mesuré en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur des millisecondes. Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. Le temps lisible par l'utilisateur qui apparaît au début du message d'audit dans le <code>audit.log</code> fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées par <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, où le T est un caractère de chaîne littérale indiquant le début du segment de temps de la date. <code>UUUUUU</code> sont des microsecondes.
ATYP	FC32	Type d'événement : identificateur à quatre caractères de l'événement en cours de consignation. Cela régit le contenu « charge utile » du message : les attributs inclus.
FINISSEUR	UI32	Version : version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet une rétrocompatibilité dans le service AMS pour traiter les messages provenant de versions antérieures de services.
RSLT	FC32	Résultat : résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

Format et exemples des messages d'audit StorageGRID

Vous trouverez des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Voici un exemple de message d'audit tel qu'il peut apparaître dans `audit.log` le fichier :

```
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 en cours d'enregistrement, ainsi que des informations sur le message d'audit lui-même.

Pour identifier l'événement enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"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. "SPUT" Représente une transaction PUT S3, qui consigne l'ingestion d'un objet dans un compartiment.

Le message d'audit suivant indique également le compartiment à partir duquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\): "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 universel coordonné (UTC) au début du message d'audit. Cette valeur est une version lisible par l'utilisateur de l'attribut ATIM du message d'audit lui-même :

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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-Jul-2014 21:17:59 UTC.

Messages d'audit et cycle de vie de l'objet

Lorsque des messages d'audit sont générés dans StorageGRID

Des messages d'audit sont générés à chaque ingestion, récupération ou suppression d'un objet. 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 par des identificateurs spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (godet), S3KY (clé), ou les deux
Liaison des opérations internes	CBID (identifiant interne de l'objet)

Calendrier des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de la grille, la taille de l'objet et les retards réseau, l'ordre des messages d'audit générés par les différents services peut varier de celui présenté dans les exemples de cette section.

Messages d'audit pour les transactions d'ingestion d'objets dans StorageGRID

Vous pouvez identifier les transactions d'ingestion de clients 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 le tableau suivant. Seuls les messages nécessaires au suivi de la transaction d'ingestion sont inclus.

Ingestion des messages d'audit S3

Code	Nom	Description	Tracé	Voir
SPUT	Transaction PUT S3	Une transaction d'entrée DE PUT S3 a été effectuée avec succès.	CBID, S3BK, S3KY	"SPUT : PUT S3"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

Exemple : ingestion d'objet S3

La série de messages d'audit ci-dessous est un exemple des messages d'audit générés et enregistrés dans le journal d'audit lorsqu'un client S3 ingère un objet à un nœud de stockage (LDR).

Dans cet exemple, la règle ILM active inclut la règle ILM Make 2 copies.



Tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de transfert S3 (SPUT) sont répertoriées.

Dans cet exemple, un compartiment S3 a déjà été créé.

SPUT : PUT S3

Le message SPUT est généré pour indiquer qu'une transaction PUT S3 a été émise pour créer un objet dans un compartiment spécifique.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"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 appliquée.

Pour les objets répliqués, le champ EMBLEMENTS inclut l'ID de nœud LDR et l'ID de volume des emplacements d'objets.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Pour les objets avec code d'effacement, le champ EMBLEMENTS inclut l'ID du profil de code d'effacement et l'ID du groupe de codes d'effacement

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Le champ PATH inclut les informations sur le bucket S3 et la clé.

```
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]]
```

Messages d'audit pour les transactions de suppression d'objets dans StorageGRID

Vous pouvez identifier les transactions de suppression 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 opération de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracé	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un compartiment.	CBID, S3KY	"SDEL : SUPPRESSION S3"

Exemple : suppression d'objet S3

Lorsqu'un client S3 supprime un objet d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.



Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de suppression S3 (SDEL) sont répertoriées.

SDEL : suppression S3

La suppression d'objet commence lorsque le client envoie une requête DeleteObject à un service LDR. Le message contient le compartiment à partir duquel vous souhaitez supprimer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_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]]
```

Messages d'audit pour les transactions de récupération d'objets dans StorageGRID

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 le tableau suivant. Seuls les messages nécessaires au suivi de la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracé	Voir
SGET	OBTENTION S3	Demande de récupération d'un objet à partir d'un compartiment.	CBID, S3BK, S3KY	"SGET : OBTENEZ S3"

Exemple : récupération d'objets S3

Lorsqu'un client S3 récupère un objet à partir d'un nœud de stockage (service LDR), un message d'audit est

génééré et enregistré dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction de récupération S3 (SGET) sont répertoriées.

SGET : OBTENEZ S3

La récupération d'objet commence lorsque le client envoie une requête GetObject à un service LDR. Le message contient le compartiment à partir duquel vous pouvez récupérer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJtlw75GBh-
O_FEW=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK(CSTR):"bucket-
anonymous"\]\[S3KY(CSTR):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP(FC32):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Si la règle de compartiment le permet, un client peut récupérer des objets de façon anonyme ou récupérer des objets à partir d'un compartiment qui est détenu par un autre compte de locataire. Le message d'audit contient des informations sur le compte du propriétaire du compartiment afin que vous puissiez suivre ces demandes anonymes et inter-comptes.

Dans l'exemple de message suivant, le client envoie une requête GetObject pour un objet stocké dans un compartiment dont il n'est pas propriétaire. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom de compte du propriétaire du compartiment, qui diffèrent de l'ID et du nom du compte du locataire enregistré dans S3AI et SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
(CSTR):"17915054115450519830"\]\[SACC(CSTR):"s3-account-
b"\]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg==" ][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI(CSTR):"4397929817
8977966408"\]\[SBAC(CSTR):"s3-account-a"\]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemple : S3 Select sur un objet

Lorsqu'un client S3 émet une requête S3 Select sur un objet, des messages d'audit sont générés et enregistrés dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction S3 Select (SelectObjectContent) sont répertoriées.

Chaque requête génère deux messages d'audit : un qui effectue l'autorisation de la requête S3 Select (le champ S3SR est défini sur « SELECT ») et une opération GET standard qui récupère les données du stockage pendant le traitement.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\": \"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messages d'audit pour les mises à jour des métadonnées des objets S3 dans StorageGRID

Des messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de la mise à jour des métadonnées S3

Code	Nom	Description	Tracé	Voir
SUPD	Métadonnées S3 mises à jour	Générées lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	"SUPD : métadonnées S3 mises à jour"

Exemple : mise à jour des métadonnées S3

L'exemple illustre la réussite d'une transaction permettant de mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 effectue une requête (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 celui-ci a été configuré comme en-tête de protocole d'audit (**Configuration > Monitoring > Audit and syslog server**). Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#).

```
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

Découvrez les types et codes de messages d'audit dans StorageGRID

Les descriptions détaillées des messages d'audit renvoyés par le système sont répertoriées dans les sections suivantes. Chaque message d'audit est d'abord répertorié

dans un tableau qui regroupe les messages associés en fonction de la classe d'activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types d'activités auditées et pour sélectionner le type souhaité de filtrage des messages d'audit.

Les messages d'audit sont également répertoriés par ordre alphabétique par leur code à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés 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 la gestion des journaux et le serveur syslog externe](#)"

Catégories de messages d'audit

Messages d'audit pour les événements système dans StorageGRID

Les messages d'audit appartenant à la catégorie d'audit du système sont utilisés pour les événements liés au système d'audit lui-même, aux États des nœuds de la grille, à l'activité des tâches à l'échelle du système (tâches de la grille) et aux opérations de sauvegarde des services.

Code	Titre et description du message	Voir
ECMC	Fragment de données manquant avec code d'effacement : indique qu'un fragment de données manquant avec code d'effacement a été détecté.	" ECMC : fragment de données avec code d'effacement manquant "
ECOC	Fragment de données avec code d'effacement corrompu : indique qu'un fragment de données avec code d'effacement corrompu a été détecté.	" ECOC : fragment de données avec code d'effacement corrompu "
EN	Échec de l'authentification de sécurité : une tentative de connexion à l'aide du protocole TLS (transport Layer Security) a échoué.	" ETAF : échec de l'authentification de sécurité "
GNRG	Enregistrement GNDS : service mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.	" GNRG : enregistrement GNDS "

Code	Titre et description du message	Voir
GNUR	Annulation de l'enregistrement du GNDS : un service s'est désinscrit du système StorageGRID.	"GNUR : non-inscription du GNDS"
GTED	Tâche de grille terminée : le service CMN a terminé le traitement de la tâche de grille.	"GTED : tâche de grille terminée"
GTST	Tâche de grille démarrée : le service CMN a commencé à traiter la tâche de grille.	"GTST : tâche de grille démarrée"
GTSU	Tâche de grille soumise : une tâche de grille a été envoyée au service CMN.	"GTSU : tâche de grille soumise"
LLST	Emplacement perdu : ce message d'audit est généré en cas de perte d'un emplacement.	"LLST : emplacement perdu"
OLST	Objet perdu : un objet demandé ne peut pas se trouver dans le système StorageGRID.	"OLST : le système a détecté un objet perdu"
AJOUTER	Désactivation de l'audit de sécurité : l'enregistrement des messages d'audit a été désactivé.	"SADD : désactivation de l'audit de sécurité"
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été restaurée.	"SADE : activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : échec de la vérification d'un bloc de contenu.	"SVRF : échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : données d'objet inattendues détectées dans le magasin d'objets.	"SVRU : Vérification du magasin d'objets inconnue"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a démarré un arrêt normal.	"SYST : arrêt du nœud"
SYSU	Node Start : service démarré, la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

Messages d'audit pour les événements de stockage d'objets dans StorageGRID

Les messages d'audit appartenant à la catégorie d'audit du stockage objet sont utilisés pour les événements liés au stockage et à la gestion d'objets au sein du système StorageGRID. Il s'agit notamment du stockage objet et des récupérations, des transferts entre nœuds grid et nœuds.



Les codes d'audit sont supprimés du produit et de la documentation, car les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour connaître les versions antérieures de SG. Par exemple "[Messages d'audit du stockage objet StorageGRID 11.8](#)", .

Code	Description	Voir
BROR	Demande de lecture seule du compartiment : un compartiment est entré ou a quitté le mode lecture seule.	"BROR : demande en lecture seule du compartiment"
CBSE	Objet Envoyer fin : l'entité source a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBSE : fin de l'envoi de l'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBRE : fin de la réception de l'objet"
CGRR	Demande de réplication multigrille : StorageGRID a tenté une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.	"CGRR : demande de réplication croisée"
EBDL	Suppression d'un compartiment vide : l'analyse ILM a supprimé un objet d'un compartiment qui supprime tous les objets (opération de compartiment vide).	"EBDL : suppression du compartiment vide"
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter la suppression d'objets).	"EBKR : demande de godet vide"
BALAYAGE	Validation d'un magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut désormais être demandé.	"SCMT : demande de validation de magasin d'objets"
SREM	Suppression du magasin d'objets : un bloc de contenu a été supprimé d'un nœud de grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

Messages d'audit pour les opérations de lecture client dans StorageGRID

Les messages d'audit de lecture du client sont consignés lorsqu'une application client S3 demande la récupération d'un objet.

Code	Description	Utilisé par	Voir
S3SL	Demande S3 Select : enregistre une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL: Demande S3 Select"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : TÊTE S3"

Messages d'audit pour les opérations d'écriture client dans StorageGRID

Les messages d'audit d'écriture du client sont consignés lorsqu'une application client S3 demande de créer ou de modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Remplacement d'objet : consigne une transaction afin de remplacer un objet par un autre.	Client S3	"OVWR : remplacement d'objet"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPR	POST S3 : consigne une transaction réussie pour restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPO : BORNE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : PUT S3"

Code	Description	Utilisé par	Voir
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment.	Client S3	"SUPD : métadonnées S3 mises à jour"

Messages d'audit de gestion StorageGRID

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : journal des demandes utilisateur.	"MGAU : message d'audit de gestion"

Messages d'audit ILM StorageGRID

Les messages d'audit appartenant à la catégorie d'audit ILM sont utilisés pour les événements liés aux opérations de gestion du cycle de vie des informations (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée de l'ILM : ce message d'audit est généré lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
LKCU	Nettoyage d'objet écrasé. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : nettoyage d'objet écrasé"
ORLM	Règles objet respectées : ce message d'audit est généré lorsque les données objet sont stockées comme spécifié par les règles ILM.	"ORLM : règles d'objet respectées"

Référence du message d'audit

Message d'audit BROR pour les requêtes de lecture seule sur les compartiments dans StorageGRID

Le service LDR génère ce message d'audit lorsqu'un compartiment passe en mode lecture seule ou quitte ce mode. Par exemple, un compartiment passe en mode lecture seule tandis que tous les objets sont en cours de suppression.

Code	Champ	Description
BKHD	UUID de compartiment	ID du compartiment.

Code	Champ	Description
BROV	Valeur de demande de lecture seule du compartiment	Que le compartiment soit en lecture seule ou qu'il quitte l'état en lecture seule (1 = lecture seule, 0 = non-lecture seule).
BROS	Motif de compartiment en lecture seule	Raison pour laquelle le compartiment est en lecture seule ou quitte l'état en lecture seule. Par exemple, emptyBucket.
S3AI	ID de compte locataire S3	ID du compte de locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

Message d'audit CBRB pour le début de la réception d'objet dans StorageGRID

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.

Code	Champ	Description
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

Message d'audit CBRE pour la fin de réception d'objet dans StorageGRID

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

Message d'audit CBSB pour l'objet send begin dans StorageGRID

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.

Code	Champ	Description
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

Message d'audit CBSE pour la fin d'envoi d'objet dans StorageGRID

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.

Code	Champ	Description
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

Message d'audit CGRR pour les demandes de réplication inter-grilles dans StorageGRID

Ce message est généré lorsque StorageGRID tente une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets. L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les requêtes de réplication multigrille couvrant une mise à niveau StorageGRID 11.7 à 11.8 peuvent avoir une taille d'objet totale inexacte.
S3AI	ID de compte locataire S3	ID du compte de locataire qui détient le compartiment à partir duquel l'objet est répliqué.
GFID	ID de connexion de fédération de grille	ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.

Code	Champ	Description
OPER	Opération CGR	Type d'opération de réplication inter-grille qui a été tentée : • 0 = objet répliqué • 1 = objet multi pièce répliqué • 2 = marqueur de suppression répliqué
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.
VSID	ID de version	ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie réussi (SUCS) ou erreur générale (GERR).

Message d'audit EBDL pour les suppressions d'objets de compartiment vides dans StorageGRID

Le scanner ILM a supprimé un objet d'un compartiment qui supprime tous les objets (en cours d'exécution d'une opération de compartiment vide).

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
RSLT	Résultat de l'opération de suppression	Résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

Message d'audit EBKR pour les requêtes de compartiment vide dans StorageGRID

Ce message indique qu'un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter de supprimer des objets).

Code	Champ	Description
BUID	UUID de compartiment	ID du compartiment.
EBJS	Configuration JSON de compartiment vide	Contient le fichier JSON représentant la configuration de compartiment vide actuelle.
S3AI	ID de compte locataire S3	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

Message d'audit ECMC pour des données à codage d'effacement manquantes dans StorageGRID

Ce message d'audit indique que le système a détecté un fragment de données avec code d'effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Nom du VCS contenant le bloc manquant.
CODE DE DIAGNOSTIC	ID de bloc	Identifiant du fragment avec code d'effacement manquant.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

Message d'audit ECOC pour des données à codage d'effacement corrompues dans StorageGRID

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Nom du VCS contenant le bloc corrompu.
VLID	ID du volume	Volume RangeDB contenant le fragment codé d'effacement corrompu.
CCID	ID de bloc	Identificateur du fragment codé d'effacement corrompu.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

Message d'audit ETAF relatif aux échecs d'authentification de sécurité dans StorageGRID

Ce message est généré lorsqu'une tentative de connexion avec TLS (transport Layer Security) a échoué.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Identifiant dépendant du service représentant l'identité de l'utilisateur distant.
RSLT	Code de motif	La raison de l'échec : SCNI : échec de l'établissement de connexion sécurisée. CERM : certificat manquant. CERT : le certificat n'était pas valide. CERE: Le certificat a expiré. CERR : le certificat a été révoqué. CSGN : la signature du certificat n'est pas valide. CSGU : le signataire de certificat était inconnu. UCRM : les informations d'identification de l'utilisateur étaient manquantes. UCRI : les informations d'identification de l'utilisateur étaient incorrectes. UCRU : les informations d'identification de l'utilisateur ont été interdites. TOUT : expiration du délai d'authentification.

Lorsqu'une connexion est établie à un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et de la logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou interdits, un message d'audit est consigné. Cela permet de rechercher des tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut être dû à une entité distante ayant une configuration incorrecte ou à des tentatives de

présentation d'informations d'identification non valides ou interdites au système. Ce message d'audit doit être surveillé pour détecter les tentatives d'accès non autorisé au système.

Message d'audit GNRG pour l'enregistrement GNDS dans StorageGRID

Le service CMN génère ce message d'audit lorsqu'un service a mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.
GNTTP	Type de périphérique	Type de périphérique du nœud de grid (par exemple BLDR pour un service LDR).
GNDV	Version du modèle de périphérique	Chaîne identifiant la version du modèle de terminal du nœud de grille dans le bundle DMDL.
GNP	Groupe	Groupe auquel appartient le nœud de la grille (dans le contexte des coûts de lien et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de la grille.

Ce message est généré chaque fois qu'un nœud de la grille met à jour son entrée dans le pack Grid Nodes.

Message d'audit GNUR pour la désinscription GNDS dans StorageGRID

Le service CMN génère ce message d'audit lorsqu'un service a des informations non enregistrées sur lui-même à partir du système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.

Message d'audit GTED pour les tâches de grille terminées dans StorageGRID

Ce message d'audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et a déplacé la tâche vers la table Historique. Si le résultat est SUC, ABRT ou ROLF, un message d'audit correspondant à la tâche de grille démarrée sera affiché. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais démarré.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche de grille tout au long de son cycle de vie. Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat de l'état final de la tâche de grille : • SUC : la tâche de grille s'est terminée avec succès. • ABRT : la tâche de grille a été interrompue sans erreur de retour arrière. • ROLF : la tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration. • ANNUL : la tâche de grille a été annulée par l'utilisateur avant son démarrage. • EXPR : la tâche de grille a expiré avant son démarrage. • IVLD : la tâche de grille n'était pas valide. • AUTH : la tâche de grille n'était pas autorisée. • DUPL : la tâche de grille a été rejetée en double.

Message d'audit GTST pour les tâches de grille démarrées dans StorageGRID

Ce message d'audit indique que le service CMN a commencé à traiter la tâche de grille spécifiée. Le message d'audit suit immédiatement le message de la tâche de grille soumise pour les tâches de grille initiées par le service interne Grid Task Submission et sélectionnées pour l'activation automatique. Pour les tâches de grille soumises dans la table en attente, ce message est généré lorsque l'utilisateur démarre la tâche de grille.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat. Ce champ n'a qu'une seule valeur : • SUC : la tâche de grille a été démarrée avec succès.

Message d'audit GTSU pour les tâches de grille soumises dans StorageGRID

Ce message d'audit indique qu'une tâche de grille a été envoyée au service CMN.

Code	Champ	Description
2	ID de tâche	Identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
TTYP	Type de tâche	Type de tâche de grille.
VER	Version de la tâche	Numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Description lisible par l'homme de la tâche de grille.
CUVES	Valide après horodatage	La première fois (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant horodatage	Dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.

Code	Champ	Description
TSRC	Source	Source de la tâche : • TXTB : la tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches Grid interne.
ACTV	Type d'activation	Type d'activation : • AUTO : la tâche de grille a été soumise pour l'activation automatique. • PEND : la tâche de grille a été envoyée dans la table en attente. C'est la seule possibilité pour la source TXTB.
RSLT	Résultat	Résultat de la soumission : • SUC : la tâche de grille a été envoyée avec succès. • ECHEC : la tâche a été déplacée directement vers la table historique.

Message d'audit IDEL pour les suppressions initiées par ILM dans StorageGRID

Ce message est généré lorsque ILM démarre le processus de suppression d'un objet.

Le message IDEL est généré dans l'une ou l'autre des situations suivantes :

- **Pour les objets dans des compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d'un objet parce que sa période de conservation a expiré (en supposant que le paramètre de suppression automatique est activé et que la conservation légale est désactivée).
- **Pour les objets dans les compartiments S3 non conformes**. Ce message est généré lorsque ILM démarre le processus de suppression d'un objet, car aucune instruction de placement dans les règles ILM actives ne s'applique actuellement à cet objet.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CMPA	Conformité : suppression automatique	Pour les objets des compartiments S3 uniquement. 0 (false) ou 1 (true), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le compartiment ne soit soumis à une conservation légale.
CMPL	Conformité : obligation légale	Pour les objets des compartiments S3 uniquement. 0 (faux) ou 1 (vrai), indiquant si le godet est actuellement en attente légale.

Code	Champ	Description
CMPR	Conformité : période de conservation	Pour les objets des compartiments S3 uniquement. Durée de conservation de l'objet en minutes.
CTME	Conformité : temps d'entrée	Pour les objets des compartiments S3 uniquement. Temps d'ingestion de l'objet. Vous pouvez ajouter la période de conservation en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENT S	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMBLEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/cl é S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	• Si un objet d'un compartiment S3 conforme est supprimé automatiquement car sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé car il n'y a plus d'instructions de placement qui s'appliquent actuellement à l'objet, ce champ affiche l'étiquette lisible par l'homme de la dernière règle ILM appliquée à l'objet.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit LKCU pour le nettoyage des objets écrasés dans StorageGRID

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui auparavant requiert un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin qui contient déjà un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet en octets.
LTYP	Type de nettoyage	<i>Usage interne uniquement.</i>
LUID	UUID d'objet supprimé	Identifiant de l'objet qui a été supprimé.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et 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	Identifiant de l'objet qui existe toujours. Cette valeur est disponible uniquement si l'objet n'a pas été supprimé.

Message d'audit LKDM pour le nettoyage des objets ayant fuité dans StorageGRID

Ce message est généré lorsqu'un morceau qui fuit a été nettoyé ou supprimé. Un bloc peut faire partie d'un objet répliqué ou d'un objet avec code d'effacement.

Code	Champ	Description
CLOC	Emplacement des blocs	Le chemin du fichier du morceau qui a fui et qui a été supprimé.
CTYP	Type de bloc	Type de bloc : ec: Erasure-coded object chunk repl: Replicated object chunk

Code	Champ	Description
LTyp	Type de fuite	Les cinq types de fuites pouvant être détectés : <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 des blocs	Heure à laquelle le morceau de fuite a été créé.
UUID	Identifiant unique universel	Identifiant de l'objet auquel appartient le bloc.
CBID	Identificateur du bloc de contenu	CBID de l'objet auquel appartient le segment divulgué.
CSIZ	Taille du contenu	Taille du bloc en octets.

Message d'audit LLST concernant les emplacements de copies d'objets perdus dans StorageGRID

Ce message est généré chaque fois qu'un emplacement pour une copie d'objet (répliquée ou avec code d'effacement) est introuvable.

Code	Champ	Description
BIL	CBID	CBID affecté.
ECPR	Profil de codage d'effacement	Pour les données d'objet avec code d'effacement. ID du profil de code d'effacement utilisé.
LTyp	Type d'emplacement	CLDI (Online) : pour les données d'objet répliquées CLEC (en ligne) : pour les données d'objet avec code d'effacement CLNL (Nearline) : pour les données d'objets répliqués archivés

Code	Champ	Description
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin d'accès à l'objet répliqué	Chemin complet vers l'emplacement du disque des données de l'objet perdu. Renvoyé uniquement lorsque LTYP a une valeur CLDI (c'est-à-dire pour les objets répliqués). Prend le formulaire <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Résultat	Toujours AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
TSRC	Déclenchement de la source	UTILISATEUR : utilisateur déclenché SYST : déclenchement du système
UUID	ID universel unique	Identifiant de l'objet affecté dans le système StorageGRID.

Message d'audit MGAU pour les requêtes API de gestion dans StorageGRID

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion. Chaque requête HTTP qui n'est pas une requête GET ou HEAD à un URI d'API valide consigne une réponse contenant le nom d'utilisateur, l'adresse IP et le type de requête à l'API. Les URI d'API non valides (tels que /api/v3-Authorise) et les demandes non valides d'URI d'API valides ne sont pas consignés.

Code	Champ	Description
MDIP	Adresse IP de destination	Adresse IP du serveur (destination).
ADNM	Nom de domaine	Nom du domaine hôte.
MPAT	CHEMIN de la demande	Le chemin de la demande.
MPQP	Paramètres de requête	Paramètres de requête pour la demande.

Code	Champ	Description
MBD	Corps de la demande	Le contenu de l'organisme de demande. Lorsque le corps de réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de réponse, elles sont extraites du corps de la demande pour les méthodes SUIVANTES : • Nom d'utilisateur et ID de compte dans POST Authorise • Nouvelle configuration de sous-réseaux dans POST /grid/grid-Networks/update • Nouveaux serveurs NTP dans POST /grid/ntp-servers/update • ID de serveur déclassés dans POST /grid/serveurs/désaffecter Remarque : les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MMD	Méthode de demande	La méthode de requête HTTP : • POST • EN • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de réponse	Le contenu de la réponse (le corps de réponse) est consigné par défaut. Remarque : les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MSIP	Adresse IP source	Adresse IP du client (source).
UUUN	URN utilisateur	URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

Message d'audit OLST pour les objets perdus détectés par le système dans StorageGRID

Ce message est généré lorsque le service DDS ne trouve aucune copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet perdu.
NON	ID du nœud	S'il est disponible, dernier emplacement direct ou proche de la ligne connue de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations sur le volume ne sont pas disponibles.
CHEMIN	Compartiment/clé S3	S'il est disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
UUID	ID universel unique	Identificateur de l'objet perdu dans le système StorageGRID.
VOLI	ID du volume	S'il est disponible, l'ID de volume du nœud de stockage pour le dernier emplacement connu de l'objet perdu.

Message d'audit ORLM pour les règles ILM respectées dans StorageGRID

Ce message est généré lorsque l'objet est stocké et copié comme spécifié par les règles ILM.



Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle de création de 2 copies par défaut si une autre règle de la stratégie utilise le filtre avancé taille d'objet.

Code	Champ	Description
BUID	Cueilleur de godet	Champ ID de compartiment. Utilisé pour les opérations internes. S'affiche uniquement si STAT est PRGD.
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CSIZ	Taille du contenu	Taille de l'objet en octets.

Code	Champ	Description
EMPLACEMENT S	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMBLEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	Étiquette lisible par l'homme donnée à la règle ILM appliquée à cet objet.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	CBID du conteneur	CBID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que pour les objets segmentés et partitionnés.
URGENCE	État	État de l'opération ILM. L'OPÉRATION ILM est terminée pour l'objet. DFER: L'objet a été marqué pour une future réévaluation ILM. PRGD : l'objet a été supprimé du système StorageGRID. NLOC : les données d'objet ne sont plus disponibles dans le système StorageGRID. Cet état peut indiquer que toutes les copies des données d'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un seul objet. Par exemple, il est émis chaque fois que l'un des événements suivants se produit :

- Les règles ILM de l'objet sont satisfaites à jamais.
- Les règles ILM de l'objet sont satisfaites pour cette époque.
- Les règles ILM ont supprimé l'objet.
- Le processus de vérification en arrière-plan détecte qu'une copie des données d'objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations associées

- ["Transactions d'ingestion d'objets"](#)
- ["Transactions de suppression d'objet"](#)

Message d'audit OVWR pour les remplacements d'objets dans StorageGRID

Ce message est généré lorsqu'une opération externe (client-demandé) provoque le remplacement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	CBID du nouvel objet.
CSIZ	Taille d'objet précédente	Taille, en octets, de l'objet à remplacer.
OCBD	Identifiant de bloc de contenu (précédent)	CBID de l'objet précédent.
UUID	ID universel unique (nouveau)	Identifiant du nouvel objet dans le système StorageGRID.
OUID	ID universel unique (précédent)	Identifiant de l'objet précédent dans le système StorageGRID.
CHEMIN	Chemin d'objet S3	Chemin d'accès à l'objet S3 utilisé pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction de remplacement d'objet. Le résultat est toujours : CMC : réussi
SGRP	Site (groupe)	S'il est présent, l'objet écrasé a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet écrasé a été ingéré.

Message d'audit S3SL pour les requêtes S3 Select dans StorageGRID

Ce message consigne une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.

Code	Champ	Description
BYSC	Octets analysés	Nombre d'octets analysés (reçus) à partir des nœuds de stockage. BYSC et BYPR sont susceptibles d'être différents si l'objet est compressé. Si l'objet est compressé, BYSC aura le nombre d'octets compressés et BYPR les octets après décompression.
MODÈLE BYPR	Octets traités	Nombre d'octets traités. Indique le nombre d'octets analysés ou traités par un travail S3 Select.
MODÈLE BYRT	Octets renvoyés	Nombre d'octets renvoyés par une tâche S3 Select au client.
RÉFÉRENTIEL	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a reçus des nœuds de stockage.
REIU	Documents renvoyés	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a renvoyé au client.
JOFI	Travail terminé	Indique si le traitement du travail S3 Select est terminé ou non. Si cette valeur est faux, le travail n'a pas pu se terminer et les champs d'erreur contiennent probablement des données. Le client a peut-être reçu des résultats partiels ou aucun résultat.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Heure d'exécution	Temps, en secondes, nécessaire à la réalisation de S3 Select Job.
GROUPE DE GESTION	Message d'erreur	Message d'erreur généré par le travail S3 Select.
QTÉ	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Erreur Stacktrace	Erreur Stacktrace générée par le travail S3 Select.
S3BK	Compartiment S3	Nom du compartiment S3.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.

Message d'audit SADD pour la désactivation de l'audit de sécurité dans StorageGRID

Ce message indique que le service d'origine (ID du nœud) a désactivé la journalisation des messages d'audit. StorageGRID ne collecte ni ne transmet plus de messages d'audit.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la journalisation était déjà activée, mais qu'elle a été désactivée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré (SADE) et la capacité de désactivation de l'audit est ensuite bloquée de manière permanente.

Message d'audit SADE pour l'activation de l'audit de sécurité dans StorageGRID

Ce message indique que le service d'origine (ID du nœud) a rétabli la journalisation des messages d'audit. StorageGRID collecte et distribue à nouveau les messages d'audit.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour activer l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la consignation a été précédemment désactivée (SADD), mais qu'elle a maintenant été restaurée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré et la fonctionnalité de désactivation de l'audit est bloquée définitivement.

Message d'audit SCMT pour les validations dans StorageGRID

Le contenu de la grille n'est pas disponible ou reconnu comme stocké tant qu'il n'a pas été engagé (c'est-à-dire qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a transmis des contrôles d'intégrité liés. Ce message est émis lorsqu'un bloc de contenu est attribué au stockage.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu engagé dans le stockage permanent.
RSLT	Code de résultat	Statut au moment où l'objet était stocké sur le disque : SUCS : objet enregistré avec succès.

Ce message signifie qu'un bloc de contenu donné a été complètement stocké et vérifié, et qu'il peut maintenant être demandé. Il peut être utilisé pour suivre le flux de données dans le système.

Message d'audit SDEL pour les transactions S3 DELETE dans StorageGRID

Lorsqu'un client S3 émet une transaction DE SUPPRESSION, une demande de suppression de l'objet ou du compartiment spécifié ou de suppression d'une sous-ressource de compartiment/objet est formulée. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
ASRS	URN de session de rôle assumé	L'identifiant unique de la session de rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.

Code	Champ	Description
ASRU	URN de rôle assumé	L'identifiant unique du rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments n'incluent pas ce champ.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande de suppression de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). x-amz-bypass-governance-retention est automatiquement inclus s'il est présent dans la demande.

Code	Champ	Description
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.

Code	Champ	Description
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UDM	Identificateur unique universel pour un marqueur de suppression	Identifiant d'un marqueur de suppression. Les messages du journal d'audit indiquent UUDM ou UUID : UUDM indique un marqueur de suppression créé à la suite d'une demande de suppression d'objet et UUID indique un objet.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SGET pour les transactions S3 GET dans StorageGRID

Lorsqu'un client S3 émet une transaction GET, une demande est formulée pour extraire un objet ou répertorier les objets dans un compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
ASRS	URN de session de rôle assumé	L'identifiant unique de la session de rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
ASRU	URN de rôle assumé	L'identifiant unique du rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. <code>`X-Forwarded-For`</code> Est automatiquement inclus s'il est présent dans la demande et si la <code>`X-Forwarded-For`</code> valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
NULLITÉ	ListObjectsV2	Une réponse v2 <i>format</i> a été demandée. Pour plus de détails, voir "AWS ListObjectsV2" . Uniquement pour les opérations GET bucket.
NHD	Nombre d'enfants	Inclut des clés et des préfixes courants. Uniquement pour les opérations GET bucket.
AU RANG	Plage lue	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette demande. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
TRNC	Tronqué ou non tronqué	Définissez sur FALSE si tous les résultats ont été renvoyés. Réglez sur vrai si d'autres résultats sont disponibles pour revenir. Uniquement pour les opérations GET bucket.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SHEA pour les opérations S3 HEAD dans StorageGRID

Lorsqu'un client S3 émet une opération 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 l'opération réussit.

Code	Champ	Description
ASRS	URN de session de rôle assumé	L'identifiant unique de la session de rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
ASRU	URN de rôle assumé	L'identifiant unique du rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet vérifié en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` 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 : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.

Code	Champ	Description
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SPOS pour les transactions S3 POST dans StorageGRID

Lorsqu'un client S3 émet une requête POST-objet, ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
ASRS	URN de session de rôle assumé	L'identifiant unique de la session de rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
ASRU	URN de rôle assumé	L'identifiant unique du rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). (Non prévu pour SPOS).
RSLT	Code de résultat	Résultat de la demande RestoreObject. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant. Réglez sur « SELECT » pour une opération S3 Select.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	Informations sur la restauration.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SPUT pour les transactions S3 PUT dans StorageGRID

Lorsqu'un client S3 émet une transaction PUT, une demande est formulée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
ASRS	URN de session de rôle assumé	L'identifiant unique de la session de rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.

Code	Champ	Description
ASRU	URN de rôle assumé	L'identifiant unique du rôle assumé. Présent uniquement lorsque la requête S3 utilise des informations d'identification de sécurité temporaires provenant d'une requête AssumeRole.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du compartiment, s'ils sont présents dans la demande (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande PUT de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande PUT de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). x-amz-bypass-governance-retention est automatiquement inclus s'il est présent dans la demande.

Code	Champ	Description
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête `x-amz-bucket-object-lock-enabled` de la demande , s'il est présent dans la demande.
LKLH	Verrouillage de l'objet en attente légale	Valeur de l'en-tête de requête <code>x-amz-object-lock-legal-hold</code> , s'il est présent dans la demande PutObject.
LKMD	Mode de conservation du verrouillage d'objet	Valeur de l'en-tête de requête <code>x-amz-object-lock-mode</code> , s'il est présent dans la demande PutObject.
LKRU	Conservation de l'objet jusqu'à la date	Valeur de l'en-tête de requête <code>x-amz-object-lock-retain-until-date</code> , s'il est présent dans la demande PutObject. Les valeurs sont limitées à 100 ans après la date d'ingestion de l'objet.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.

Code	Champ	Description
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ID ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations CompleteMultipartUpload. Indique que toutes les pièces ont été téléchargées et assemblées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.
VSST	Etat de gestion des versions	Nouvel état de gestion des versions d'un compartiment. Deux États sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

Message d'audit SREM pour la suppression d'un objet store dans StorageGRID

Ce message est émis lorsque le contenu est supprimé du stockage persistant et n'est plus accessible via des API régulières.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu supprimé du stockage permanent.
RSLT	Code de résultat	Indique le résultat des opérations de suppression de contenu. La seule valeur définie est : SUCS : contenu supprimé du stockage persistant

Ce message d'audit signifie qu'un bloc de contenu donné a été supprimé d'un nœud et ne peut plus être demandé directement. Le message peut être utilisé pour suivre le flux de contenu supprimé dans le système.

Message d'audit SUPD pour les mises à jour des métadonnées S3 dans StorageGRID

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées pour un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de requête HTTP de contrôle de cohérence, s'il est présent dans la demande, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SVRF pour les échecs de vérification du stockage d'objets dans StorageGRID

Ce message est émis chaque fois qu'un bloc de contenu échoue au processus de vérification. Chaque fois que les données d'objet répliqué sont lues ou écrites sur le disque, plusieurs vérifications et vérifications d'intégrité sont effectuées pour s'assurer que les données envoyées à l'utilisateur requérant sont identiques aux données initialement ingérées sur le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données d'objet répliqué corrompues pour les empêcher d'être récupérées à nouveau.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu qui a échoué à la vérification.

Code	Champ	Description
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : échec de la vérification du code d'authentification du message basé sur le hachage (HMAC). EHSR : hachage de contenu crypté inattendu. PHSR : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier de disque. DERR : erreur disque. FNAM : nom de fichier incorrect.



Ce message doit être surveillé de près. Les défaillances de vérification de contenu peuvent indiquer des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, reportez-vous à la valeur du champ ID du module. Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire la vérification en arrière-plan et STOR indique que le message a été déclenché par la récupération du contenu.

Message d'audit SVRU pour un contenu de magasin d'objets inconnu dans StorageGRID

Le composant de stockage du service LDR analyse en continu toutes les copies des données objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliqué est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.



Le message d'audit SVRU: Object Store Verify Unknown doit être suivi de près. Cela signifie que des copies inattendues de données objet ont été détectées dans le magasin d'objets. Cette situation doit être examinée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des défaillances matérielles imminentes.

Message d'audit SYSD pour les arrêts de nœuds en douceur dans StorageGRID

Lorsqu'un service est arrêté avec élégance, ce message est généré pour indiquer que l'arrêt a été demandé. Généralement, ce message est envoyé uniquement après un redémarrage ultérieur, car la file d'attente des messages d'audit n'est pas effacée avant l'arrêt. Recherchez le message SYST, envoyé au début de la séquence d'arrêt, si le service n'a pas redémarré.

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

Message d'audit SYST pour l'arrêt d'un nœud dans StorageGRID

Lorsqu'un service est arrêté correctement, ce message est généré pour indiquer que l'arrêt a été demandé et que le service a entamé sa séquence d'arrêt. SYST peut être utilisé pour déterminer si l'arrêt a été demandé, avant que le service ne soit redémarré (contrairement à SYSD, qui est généralement envoyé après le redémarrage du service).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

Message d'audit SYSU pour le nœud démarre dans StorageGRID

Lors du redémarrage d'un service, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système a été arrêté proprement. DSDN : le système n'a pas été arrêté complètement. VRGN : le système a été démarré pour la première fois après l'installation du serveur (ou la réinstallation).

Le message n'indique pas si le serveur hôte a été démarré, seul le service de génération de rapports. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant le fonctionnement (étant donné que la nature distribuée du système StorageGRID peut masquer ces défaillances). Server Manager redémarre automatiquement un service en panne.

Augmentez la capacité ou les fonctionnalités de votre système StorageGRID

Découvrez comment étendre votre système StorageGRID

Découvrez comment étendre votre système StorageGRID pour augmenter sa capacité ou ses fonctionnalités sans interrompre son fonctionnement. Vous pouvez ajouter des volumes de stockage aux nœuds de stockage existants, ajouter de nouveaux nœuds de grille à un site existant ou ajouter un nouveau site.

Avant de développer 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 ou d'extension. "[Vérifier les travaux de réparation des données](#)".

Une extension StorageGRID vous permet d'ajouter :

- Des volumes de stockage vers des nœuds de stockage
- Nouveaux nœuds grid sur un site existant
- Tout un nouveau site

La raison pour laquelle vous exécutez l'extension détermine le nombre de nouveaux nœuds de chaque type que vous devez ajouter et l'emplacement de ces nouveaux nœuds. Par exemple, les exigences en matière de nœuds sont différentes si vous effectuez une extension pour augmenter la capacité de stockage, ajouter de la capacité des métadonnées ou ajouter de la redondance ou de nouvelles fonctionnalités.

Suivez les étapes pour le type d'extension que vous effectuez :

Ajouter des nœuds grid

1. Suivez les étapes ["ajout de nœuds grid à un site existant"](#) de .
2. ["Mettez à jour les sous-réseaux"](#).
3. Déploiement des nœuds grid :
 - ["Appliances"](#)
 - ["VMware"](#)
 - ["Linux"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#) .

1. ["Effectuer l'extension"](#).
2. ["Configurez le système développé"](#).

Ajout de volumes de stockage

Suivez les étapes ["Ajout de volumes de stockage aux nœuds de stockage"](#) de .

Ajouter un site

1. Suivez les étapes ["Ajout d'un site"](#) de .
2. ["Mettez à jour les sous-réseaux"](#).
3. Déploiement des nœuds grid :
 - ["Appliances"](#)
 - ["VMware"](#)
 - ["Linux"](#)



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp \(IMT\)"](#) .

1. ["Effectuer l'extension"](#).
2. ["Configurez le système développé"](#).

Planification de l'expansion

Planification de l'extension des données répliquées dans StorageGRID

Si la règle de gestion du cycle de vie des informations (ILM) de votre déploiement inclut une règle qui crée des copies répliquées des objets, vous devez tenir compte de la quantité de stockage à ajouter et de l'emplacement où ajouter les nouveaux volumes ou nœuds de stockage.

Pour savoir où ajouter du stockage, consultez les règles ILM qui créent des copies répliquées. Si les règles ILM créent au moins deux copies d'objet, prévoyez d'ajouter du stockage à chaque emplacement où les copies d'objet sont créées. À titre d'exemple simple, si vous disposez d'une grille à deux sites et d'une règle ILM pour créer une copie d'objet sur chaque site, vous devez ["ajouter du stockage"](#) accéder à chaque site pour

augmenter la capacité objet globale de la grille. Pour plus d'informations sur la réplication d'objet, reportez-vous à la section ["Qu'est-ce que la réplication"](#).

Pour des raisons de performance, essayez de préserver l'équilibre entre la capacité de stockage et la puissance de calcul entre les sites. Pour cet exemple, vous devez ajouter le même nombre de nœuds de stockage à chaque site ou des volumes de stockage supplémentaires sur chaque site.

Si vous disposez d'une règle ILM plus complexe qui comprend des règles permettant de placer les objets à différents emplacements en fonction de critères tels que le nom de compartiment ou des règles qui modifient les emplacements des objets au fil du temps, votre analyse des emplacements de stockage requis pour l'extension sera similaire, mais plus complexe.

La vitesse à laquelle la capacité de stockage globale est consommée peut vous aider à déterminer la quantité de stockage à ajouter lors de l'extension et les moments où il faut ajouter de l'espace de stockage. Vous pouvez utiliser le Gestionnaire de grille pour ["surveillez et tracez la capacité de stockage"](#).

Lorsque vous planifiez le calendrier d'une extension, n'oubliez pas de prendre en compte le temps nécessaire pour acquérir et installer un stockage supplémentaire. Pour simplifier la planification de l'extension, envisagez d'ajouter des nœuds de stockage lorsque les nœuds de stockage existants atteignent 70 % de leur capacité.

Planification de l'extension des données à codage d'effacement (EC) dans StorageGRID

Si votre règle ILM comprend une règle qui effectue des copies avec code d'effacement, vous devez prévoir où ajouter du stockage, et quand ajouter de la capacité de stockage. La quantité de stockage que vous ajoutez, et la durée de l'ajout peut affecter la capacité de stockage utilisable de la grille.

La première étape de la planification d'une extension de stockage consiste à examiner les règles de la règle ILM qui créent des objets avec code d'effacement. Étant donné que StorageGRID crée des fragments $k+m$ pour chaque objet avec code d'effacement et stocke chaque fragment sur un nœud de stockage différent, vous devez vous assurer qu'au moins $k+m$ les nœuds de stockage disposent d'espace pour les nouvelles données avec code d'effacement après l'extension. Si le profil de code d'effacement assure la protection contre la perte du site, vous devez ajouter de l'espace de stockage à chaque site. Pour plus d'informations sur les profils de code d'effacement, reportez-vous à la section ["Que sont les schémas de code d'effacement"](#).

Le nombre de nœuds à ajouter dépend également de la totalité des nœuds existants lors de l'extension.

Recommandations générales pour l'ajout de capacité de stockage pour les objets avec code d'effacement

Pour éviter les calculs détaillés, vous pouvez ajouter deux nœuds de stockage par site lorsque les nœuds de stockage existants atteignent 70 % de capacité.

Cette recommandation générale donne des résultats raisonnables dans le cadre d'un large éventail de schémas de codage d'effacement pour les grilles à site unique et pour les grilles où le codage d'effacement assure la protection de la perte au niveau du site.

Pour mieux comprendre les facteurs qui ont conduit à cette recommandation ou pour élaborer un plan plus précis pour votre site, voir ["Considérations relatives au rééquilibrage des données avec code d'effacement"](#). Pour obtenir des recommandations personnalisées et optimisées selon votre situation, contactez votre consultant en services professionnels NetApp.

Découvrez le rééquilibrage EC après l'extension de StorageGRID.

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 code d'effacement si vous ne pouvez pas ajouter suffisamment de nœuds de stockage pour le modèle de code d'effacement que vous utilisez.

Après avoir passé en revue ces considérations, effectuez l'extension, puis passez à l' ["Rééquilibrent les données codées après l'ajout de nœuds de stockage"](#) pour exécuter la procédure.

Qu'est-ce que le rééquilibrage EC ?

Le rééquilibrage EC est une procédure StorageGRID qui peut être requise après l'extension d'un nœud de stockage. La procédure est exécutée en tant que script de ligne de commande à partir du nœud d'administration principal. Lorsque vous exécutez la procédure de rééquilibrage EC, StorageGRID redistribue des fragments avec code d'effacement entre les nœuds de stockage existants et nouvellement ajoutés sur un site.

La procédure de rééquilibrage de la ce :

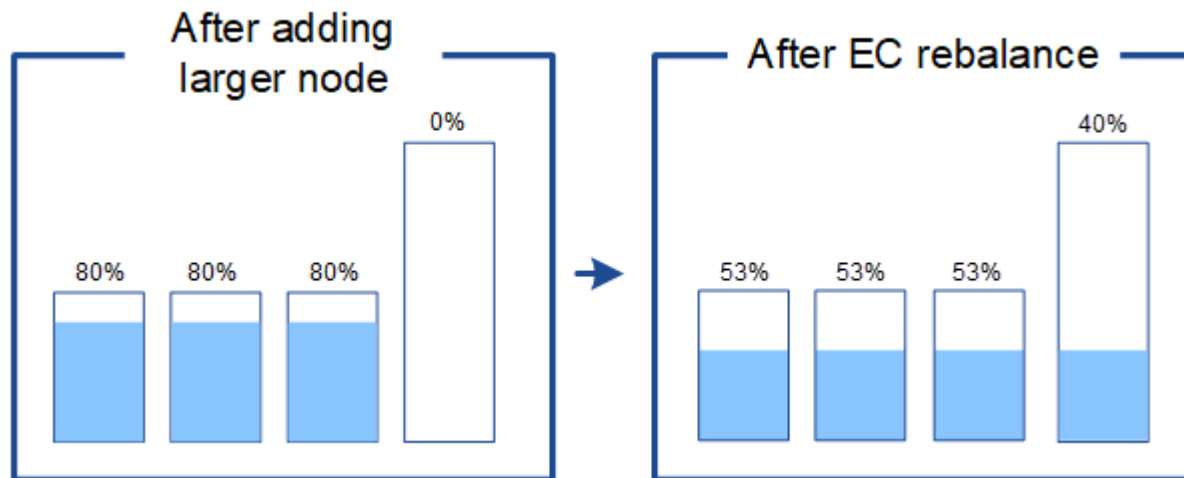
- Seul le déplacement des données d'objet avec code d'effacement Il ne déplace pas les données d'objet répliqué.
- Redistribue les données au sein d'un site. Il ne déplace pas les données entre les sites.
- Redistribue les données entre tous les nœuds de stockage du site. Elle ne rerépartit pas les données au sein des volumes de stockage.
- Le système tente de répartir les octets de données afin que chaque nœud dispose du même espace utilisable. Les nœuds contenant davantage de données répliquées pourraient stocker moins de données à codage d'effacement une fois le rééquilibrage terminé.
- Répartit uniformément l'espace utilisable entre les nœuds de stockage sans tenir compte des capacités relatives de chaque nœud. Les données répliquées sont incluses dans le calcul.
- La procédure de rééquilibrage est considérée comme terminée si elle ne peut plus déplacer de données à codage d'effacement, même si l'espace utilisable n'est toujours pas réparti uniformément.
- Ne distribuera pas les données à codage d'effacement aux nœuds de stockage remplis à plus de 80 % ni aux nœuds de stockage contenant uniquement des métadonnées.
- Risque de diminuer les performances des opérations ILM et des opérations client S3 lorsqu'elles s'exécutent—des ressources supplémentaires sont nécessaires pour redistribuer les fragments de code d'effacement.

Lorsque la procédure de rééquilibrage EC est terminée :

- Les données avec code d'effacement auront été transférées des nœuds de stockage disposant de moins d'espace disponible vers des nœuds de stockage disposant de plus d'espace disponible.
- Les données protégées des objets avec code d'effacement restent les mêmes.
- Les valeurs utilisées (%) peuvent différer d'un nœud de stockage à un autre, et ce pour deux raisons :
 - Les copies d'objet répliquées continueront à consommer de l'espace sur les nœuds existants—la procédure de rééquilibrage EC ne déplace pas les données répliquées.
 - Les nœuds de plus grande capacité peuvent être relativement moins remplis que les nœuds de plus

petite capacité, même si tous les nœuds finissent par disposer d'une quantité d'espace utilisable à peu près identique.

Par exemple, avec un schéma de codage d'effacement 2+1, supposons que trois nœuds de 200 To soient chacun remplis à 80 % ($200 \times 0,8 = 160$ To par nœud, soit 480 To pour le site). Si vous ajoutez un nœud de 400 To et exécutez la procédure de rééquilibrage, tous les anciens nœuds auront désormais approximativement la même quantité de données codées par effacement (106,66 To ou 53 % d'utilisation). Le nouveau nœud aura 160 To de données, soit 40 % d'utilisation. Dans ce cas, le pourcentage d'utilisation du nœud le plus volumineux sera inférieur à celui des nœuds les plus petits. La procédure de rééquilibrage s'achève avant que l'espace utilisable ne soit équilibré, car il n'est plus possible de déplacer de données codées par effacement sans enfreindre les contraintes du schéma de codage d'effacement.



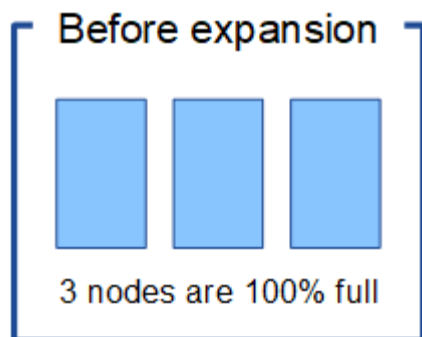
Quand rééquilibrer les données avec code d'effacement

La procédure de rééquilibrage EC redistribue les données codées par effacement existantes pour garantir que les nœuds ne deviennent pas ou ne restent pas pleins. La procédure permet de garantir que le codage EC peut continuer sur le site.

Exécutez la procédure de rééquilibrage lorsqu'il existe un biais préoccupant dans la distribution des données sur un site et que le site stocke principalement des données EC (puisque les données répliquées ne peuvent pas être déplacées par rééquilibrage).

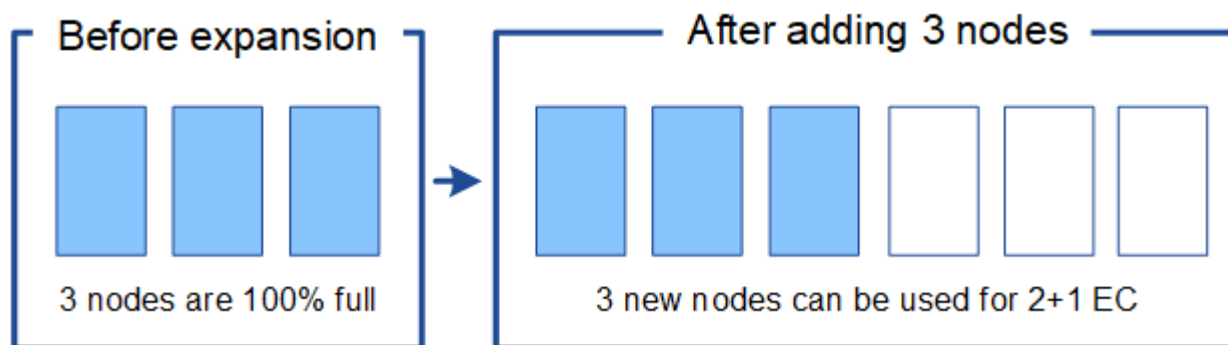
Prenons le scénario suivant :

- StorageGRID s'exécute sur un seul site, qui contient trois nœuds de stockage.
- La règle ILM utilise une règle de code d'effacement 2+1 pour tous les objets de plus de 1.0 Mo et une règle de réplication à 2 copies pour les objets plus petits.
- Tous les nœuds de stockage sont devenus complètement pleins. L'alerte **Low Object Storage** a été déclenchée au niveau de gravité principal.



Le rééquilibrage n'est pas nécessaire si vous ajoutez suffisamment de nœuds

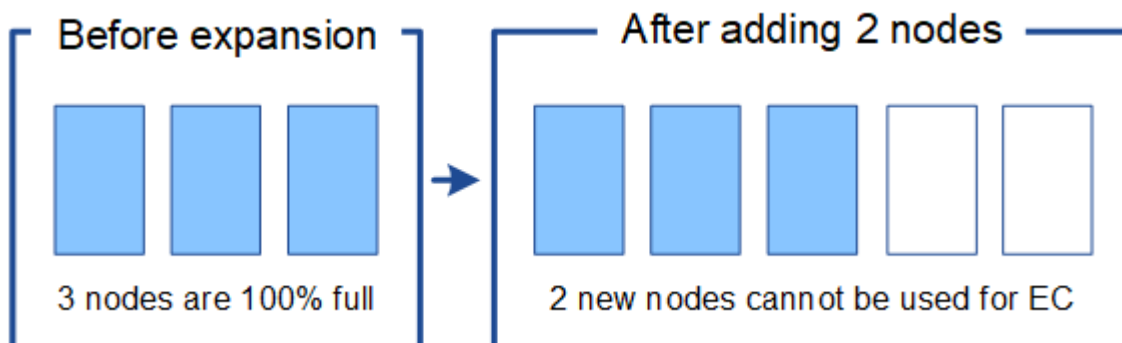
Pour savoir quand le rééquilibrage EC n'est pas nécessaire, supposons que vous ayez ajouté trois (ou plus) nouveaux nœuds de stockage. Dans ce cas, vous n'avez pas besoin d'effectuer le rééquilibrage EC. Les nœuds de stockage d'origine resteront pleins, mais les nouveaux objets utiliseront désormais les trois nouveaux nœuds pour le code d'effacement 2+1—les deux fragments de données et le fragment de parité peuvent chacun être stockés sur un nœud différent.



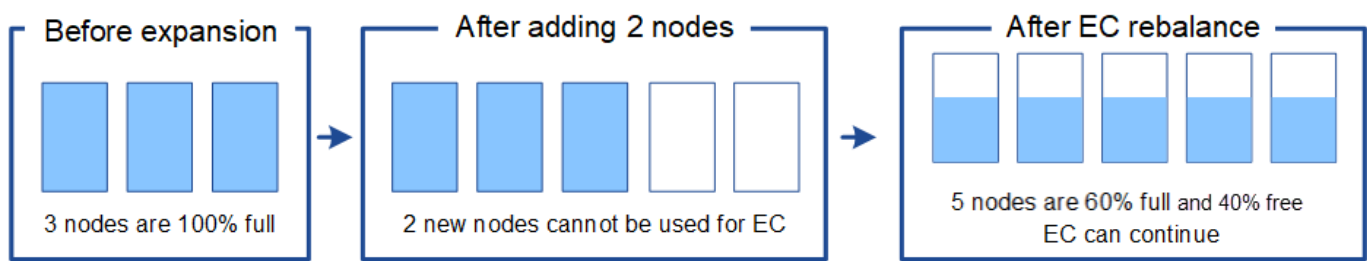
Dans ce cas, vous pouvez exécuter la procédure de rééquilibrage de l'effacement, mais le déplacement des données existantes avec code d'effacement réduit temporairement les performances de la grille, ce qui peut avoir un impact sur les opérations client.

Vous devez rééquilibrer la capacité si vous ne pouvez pas ajouter suffisamment de nœuds

Pour savoir quand un rééquilibrage EC est nécessaire, supposons que vous ne pouvez ajouter que deux nœuds de stockage au lieu de trois. Étant donné que le modèle 2+1 requiert au moins trois nœuds de stockage pour disposer d'espace disponible, les nœuds vides ne peuvent pas être utilisés pour les nouvelles données avec code d'effacement.



Pour exploiter les nouveaux nœuds de stockage, vous devez exécuter la procédure de rééquilibrage EC. Lorsque cette procédure s'exécute, StorageGRID redistribue les données à codage d'effacement et les fragments de parité existants afin que l'espace utilisable soit réparti équitablement entre tous les nœuds de stockage du site. Dans cet exemple, une fois la procédure de rééquilibrage EC terminée, les cinq nœuds sont désormais remplis à 60 % avec 40 % d'espace utilisable, et l'ingestion d'objets peut se poursuivre selon le schéma de codage d'effacement 2+1 sur tous les nœuds de stockage.



Recommandations pour le rééquilibrage de la ce

NetApp exige un rééquilibrage de l'EC si l'ensemble des affirmations suivantes est vrai :

- Vous utilisez le code d'effacement pour vos données d'objet.
- L'alerte **Low Object Storage** a été déclenchée pour un ou plusieurs nœuds de stockage d'un site, ce qui indique que les nœuds sont pleins à 80 % ou plus.
- Vous ne pouvez pas ajouter suffisamment de nœuds de stockage pour le schéma de code d'effacement utilisé. Voir "[Ajoutez de la capacité de stockage pour les objets avec code d'effacement](#)".
- Vos clients S3 peuvent tolérer une performance moindre pour leurs opérations d'écriture et de lecture pendant que la procédure de rééquilibrage de l'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 peuvent tolérer des performances moins élevées pour leurs opérations d'écriture et de lecture pendant que la procédure de rééquilibrage EC est en cours d'exécution.

Interaction entre la procédure de rééquilibrage EC et d'autres tâches de maintenance

Vous ne pouvez pas effectuer certaines procédures de maintenance en même temps que vous exécutez la procédure de rééquilibrage EC.

Procédure	Autorisé pendant la procédure de rééquilibrage EC ?
Procédures EC de rééquilibrage supplémentaires	Non Vous ne pouvez exécuter qu'une seule procédure de rééquilibrage EC à la fois.

Procédure	Autorisé pendant la procédure de rééquilibrage EC ?
Procédure de mise hors service	Non
Tâche de réparation des données EC	• Vous ne pouvez pas démarrer une procédure de déclassement ou de réparation de données EC pendant que la procédure de rééquilibrage EC est en cours d'exécution. • Vous ne pouvez pas démarrer la procédure de rééquilibrage EC lorsque la procédure de déclassement du nœud de stockage ou de réparation de données EC est en cours d'exécution.
Procédure d'expansion	Non Si vous devez ajouter de nouveaux nœuds de stockage dans une extension, exécutez la procédure de rééquilibrage de l'EC après avoir ajouté tous les nouveaux nœuds.
Procédure de mise à jour	Non Si vous devez mettre à niveau le logiciel StorageGRID, effectuez la procédure de mise à niveau avant ou après l'exécution de la procédure de rééquilibrage EC. Si nécessaire, vous pouvez mettre fin à la procédure EC Rebalance pour effectuer une mise à niveau logicielle.
Procédure de clonage des nœuds d'appliance	Non Si vous devez cloner un nœud de stockage de l'appliance, exécutez la procédure de rééquilibrage EC après avoir ajouté le nouveau nœud.
Procédure de correctif	Oui. Vous pouvez appliquer un correctif StorageGRID pendant l'exécution de la procédure EC Rérééquilibrage.
Autres procédures de maintenance	Non Vous devez arrêter la procédure de rééquilibrage EC avant d'exécuter d'autres procédures de maintenance.

La façon dont ce rééquilibrage interagit avec ILM

Pendant l'exécution de la procédure de rééquilibrage EC, évitez d'apporter des modifications au ILM susceptibles de modifier l'emplacement des objets avec code d'effacement existants. Par exemple, ne commencez pas à utiliser une règle ILM dont le profil de code d'effacement est différent. Si vous devez effectuer de telles modifications ILM, vous devez mettre fin à la procédure de rééquilibrage EC.

directives d'expansion

Instructions pour l'ajout de capacité d'objets dans StorageGRID

Pour étendre la capacité de stockage objet de votre système StorageGRID, ajoutez des volumes de stockage aux nœuds de stockage existants ou ajoutez de nouveaux nœuds de stockage aux sites existants. Vous devez ajouter de la capacité de stockage qui répond aux besoins de votre stratégie de gestion du cycle de vie des informations (ILM).

Instructions d'ajout de volumes de stockage

Avant d'ajouter des volumes de stockage à des nœuds de stockage existants, consultez les consignes et limites suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand ["ajout de volumes de stockage"](#) augmenter le stockage disponible pour ["objets répliqués"](#) ou ["objets avec code d'effacement"](#).
- L'ajout de volumes de stockage ne permet pas d'augmenter la capacité de métadonnées du système, car les métadonnées d'objet sont stockées uniquement sur le volume 0.
- Chaque nœud de stockage logiciel peut prendre en charge un maximum de 48 volumes de stockage. Si vous avez besoin d'ajouter de la capacité, vous devez ajouter des nœuds de stockage.
- Vous pouvez ajouter un ou deux tiroirs d'extension à chaque appliance SG6060. Chaque tiroir d'extension ajoute 16 volumes de stockage. Une fois les deux tiroirs d'extension installés, le SG6060 peut prendre en charge un total de 48 volumes de stockage.
- Vous pouvez ajouter un ou deux tiroirs d'extension à chaque appliance SG6160. Chaque tiroir d'extension ajoute 60 volumes de stockage. Une fois les deux tiroirs d'extension installés, le SG6160 peut prendre en charge un total de 180 volumes de stockage.
- Vous ne pouvez pas ajouter de volumes de stockage à une autre appliance de stockage.
- Vous ne pouvez pas augmenter la taille d'un volume de stockage existant.
- Vous ne pouvez pas ajouter de volumes de stockage à un nœud de stockage en même temps que vous effectuez une mise à niveau du système, une opération de restauration ou une autre extension.

Une fois que vous avez décidé d'ajouter des volumes de stockage et que vous avez déterminé les nœuds de stockage à étendre pour répondre à la règle ILM, suivez les instructions relatives à votre type de nœud de stockage :

- Pour ajouter une ou deux tiroirs d'extension à une appliance de stockage SG6060, accédez à ["Ajout du tiroir d'extension au SG6060 déployé"](#).
- Pour ajouter un ou deux tiroirs d'extension à une appliance de stockage SG6160, rendez-vous sur le site ["Ajout du tiroir d'extension au SG6160 déployé"](#)
- Pour un nœud logiciel, suivez les instructions de ["Ajout de volumes de stockage aux nœuds de stockage"](#).

Instructions sur l'ajout de nœuds de stockage

Avant d'ajouter des nœuds de stockage à des sites existants, consultez les consignes et limites suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand ajouter des nœuds de stockage afin d'augmenter le stockage disponible pour ["objets répliqués"](#) ou ["objets avec code d'effacement"](#).
- Vous ne devez pas ajouter plus de 10 nœuds de stockage en une seule procédure d'extension.
- Vous pouvez ajouter des nœuds de stockage à plusieurs sites en une seule procédure d'extension.

- Vous pouvez ajouter des nœuds de stockage et d'autres types de nœuds en une seule procédure d'extension.
- Avant de démarrer la procédure d'extension, vous devez vérifier que toutes les opérations de réparation des données effectuées dans le cadre d'une restauration sont terminées. Voir ["Vérifier les travaux de réparation des données"](#).
- Si vous devez supprimer des nœuds de stockage avant ou après une extension, vous ne devez pas désaffecter plus de 10 nœuds de stockage dans une procédure de nœud de mise hors service unique.
- Ajoutez suffisamment de nœuds de stockage pour maintenir les performances d'E/S de stockage sous-jacentes. Les opérations d'écriture seront réparties entre les nœuds de stockage en fonction de la capacité de stockage disponible. Si les nœuds de stockage étendus disposent d'une capacité de stockage disponible nettement supérieure, ces nœuds recevront beaucoup plus d'écritures. En particulier, lorsque les nœuds de stockage existants sont presque pleins, les nouvelles écritures s'appuieront uniquement sur les nœuds de stockage étendus. Les opérations de lecture et de suppression seront gérées en fonction de votre charge de travail spécifique.

Instructions relatives au service ADC sur les nœuds de stockage

Lors de la configuration de l'extension, vous devez choisir d'inclure le service contrôleur de domaine d'administration (ADC) sur chaque nouveau nœud de stockage. Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau.

- Vous pouvez ["déplacer le service ADC d'un nœud de stockage à un autre sur le même site"](#).
- Le système StorageGRID nécessite qu'un ["Quorum des services ADC"](#) soit disponible sur chaque site et à tout moment.
- Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC.
- Il est déconseillé d'ajouter le service ADC à chaque nœud de stockage. L'inclusion d'un trop grand nombre de services ADC peut provoquer des ralentissements en raison de l'augmentation de la quantité de communication entre les nœuds.
- Une seule grille ne doit pas comporter plus de 48 nœuds de stockage avec le service ADC. Cela équivaut à 16 sites avec trois services ADC sur chaque site.
- En général, lorsque vous sélectionnez le paramètre **Service ADC** pour un nouveau nœud, vous devez sélectionner **Automatique**. Sélectionnez **Oui** uniquement si le nouveau nœud remplace un autre nœud de stockage qui inclut le service ADC. Étant donné que vous ne pouvez pas désactiver un nœud de stockage s'il reste trop peu de services ADC, la sélection de **Oui** garantit qu'un nouveau service ADC est disponible avant la suppression de l'ancien service.

Instructions pour l'ajout de capacité de métadonnées dans StorageGRID

Pour assurer la disponibilité de l'espace adéquat pour les métadonnées des objets, vous devez effectuer une procédure d'extension afin d'ajouter de nouveaux nœuds de stockage sur chaque site.

StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume 0 de chaque nœud de stockage. Trois copies de toutes les métadonnées d'objet sont conservées sur chaque site, réparties de manière homogène entre tous les nœuds de stockage.

Vous pouvez utiliser Grid Manager pour surveiller la capacité des métadonnées des nœuds de stockage et estimer la vitesse de consommation de la capacité des métadonnées. En outre, l'alerte **stockage de métadonnées faible** est déclenchée pour un nœud de stockage lorsque l'espace de métadonnées utilisé atteint certains seuils.

La capacité des métadonnées d'objet d'une grille peut être consommée plus rapidement que la capacité de stockage objet, selon l'utilisation de la grille. Par exemple, si vous ingérez d'importants volumes d'objets de petite taille ou si vous ajoutez de grandes quantités de métadonnées ou de balises utilisateur aux objets, vous devrez ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage objet reste suffisante.

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

- ["Gérer le stockage des métadonnées d'objet"](#)
- ["Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage"](#)

Instructions d'augmentation de la capacité des métadonnées

Avant d'ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, consultez les directives et les limites suivantes :

- En supposant une capacité de stockage objet suffisante, l'augmentation de l'espace disponible pour les métadonnées d'objet augmente le nombre d'objets que vous pouvez stocker dans votre système StorageGRID.
- Vous pouvez augmenter la capacité des métadonnées d'une grille en ajoutant un ou plusieurs nœuds de stockage à chaque site.
- L'espace réel réservé pour les métadonnées d'objet sur un nœud de stockage donné dépend de l'option de stockage de l'espace réservé aux métadonnées (paramètre pour tout le système), de la quantité de RAM allouée au nœud et de la taille du volume 0 du nœud.
- Il est impossible d'augmenter la capacité des métadonnées en ajoutant des volumes de stockage aux nœuds de stockage existants, car les métadonnées ne sont stockées que sur le volume 0.
- L'ajout d'un nouveau site ne permet pas d'augmenter la capacité des métadonnées.
- StorageGRID conserve trois copies de toutes les métadonnées d'objets sur chaque site. C'est pourquoi la capacité de métadonnées de votre système est limitée par la capacité de métadonnées de votre plus petit site.
- Lorsque vous ajoutez de la capacité des métadonnées, vous devez ajouter le même nombre de nœuds de stockage à chaque site.

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

- Avec les appliances StorageGRID, les nœuds de métadonnées uniquement peuvent être configurés sur des appliances SGF6112 avec douze disques de 1.9 To ou douze disques de 3.8 To.
- Lors de l'utilisation de nœuds logiciels, les ressources de nœuds de métadonnées uniquement doivent correspondre aux ressources existantes des nœuds de stockage. Par exemple :
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds exclusivement basés sur des métadonnées logicielles doivent respecter la configuration minimale suivante :
 - 128 GO DE RAM
 - Processeur 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 ; les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

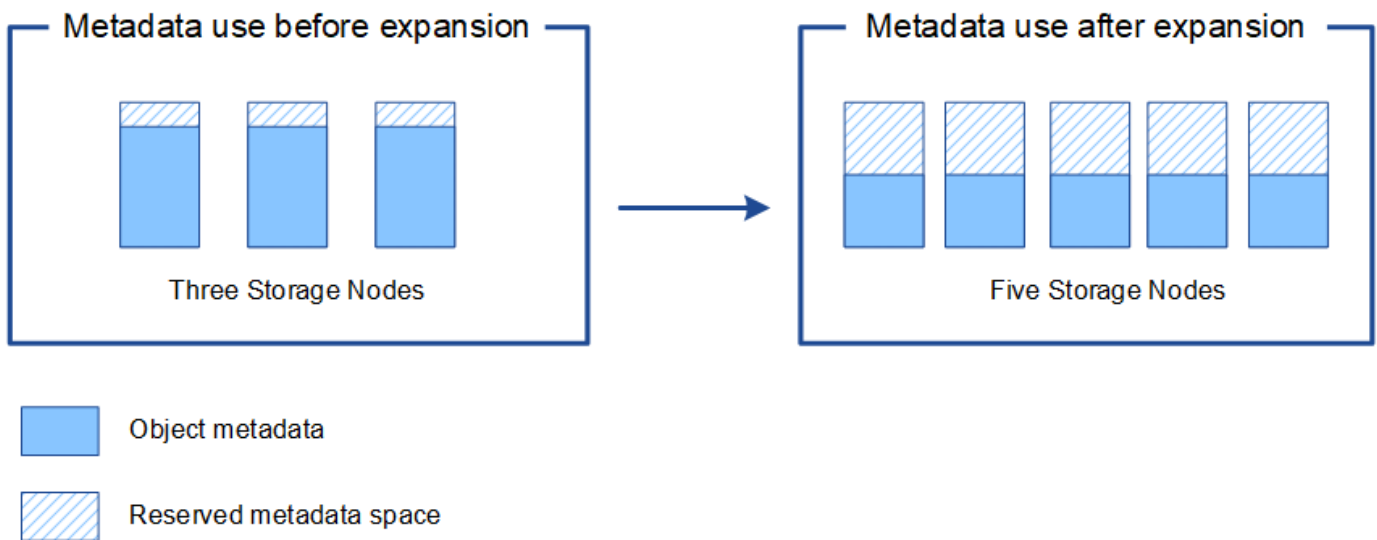
Voir la ["Description de l'espace réservé aux métadonnées"](#).

Comment les métadonnées sont redistribuées lorsque vous ajoutez des nœuds de stockage

Lorsque vous ajoutez des nœuds de stockage dans une extension, StorageGRID redistribue les métadonnées de l'objet vers les nouveaux nœuds de chaque site, ce qui augmente la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise.

La figure suivante montre comment StorageGRID redistribue les métadonnées d'objet lorsque vous ajoutez des nœuds de stockage dans une extension. La partie gauche de la figure représente le volume 0 de trois nœuds de stockage avant toute extension. Les métadonnées consomment une portion relativement importante de l'espace disponible de métadonnées de chaque nœud et l'alerte **stockage de métadonnées faible** a été déclenchée.

La partie droite de la figure montre comment les métadonnées existantes sont redistribuées après deux nœuds de stockage ajoutés au site. La quantité de métadonnées sur chaque nœud a diminué, l'alerte **stockage de métadonnées faible** n'est plus déclenchée et l'espace disponible pour les métadonnées a augmenté.



Instructions pour l'ajout de nœuds de grille dans StorageGRID

Vous pouvez ajouter de la redondance ou des fonctionnalités supplémentaires à un système StorageGRID en ajoutant de nouveaux nœuds grid à des sites existants.

Par exemple, vous pouvez choisir d'ajouter des nœuds de passerelle à utiliser dans un groupe haute disponibilité (HA) ou d'ajouter un nœud d'administration sur un site distant pour permettre la surveillance à l'aide d'un nœud local.

Vous pouvez ajouter un ou plusieurs des types de nœuds suivants à un ou plusieurs sites existants au cours d'une seule opération d'extension :

- Nœuds d'administration non primaires

- Nœuds de stockage
- Nœuds de passerelle

Lorsque vous préparez l'ajout de nœuds grid, tenez compte des limites suivantes :

- Le nœud d'administration principal est déployé lors de l'installation initiale. Vous ne pouvez pas ajouter de nœud d'administration principal pendant une extension.
- Vous pouvez ajouter des nœuds de stockage et d'autres types de nœuds dans la même extension.
- Lorsque vous ajoutez des nœuds de stockage, vous devez planifier soigneusement le nombre et l'emplacement des nouveaux nœuds. Voir ["Instructions d'ajout de capacité d'objet"](#).
- Si l'option **Définir 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 ["modifiez le paramètre de sécurité du nouveau nœud"](#) et à ["configurez les terminaux d'équilibrage de charge"](#).

Instructions pour l'ajout d'un nouveau site dans StorageGRID

Vous pouvez étendre votre système StorageGRID en ajoutant un nouveau site.

Instructions pour l'ajout d'un site

Avant d'ajouter un site, vérifiez les exigences et limites suivantes :

- Vous ne pouvez ajouter qu'un site par opération d'extension.
- Vous ne pouvez pas ajouter de nœuds grid à un site existant dans le cadre d'une même extension.
- Chaque site doit comporter au moins trois nœuds de stockage. Il peut s'agir de n'importe quelle combinaison de nœuds de stockage combinés et de nœuds de stockage de métadonnées uniquement. S'il y a plus de trois nœuds de stockage, il peut s'agir de n'importe quelle combinaison de nœuds de stockage combinés, de nœuds de stockage de métadonnées uniquement et de nœuds de stockage de données uniquement, à condition que trois services ADC soient disponibles. Pour plus d'informations, consultez ["Nœuds de stockage requis par grille et par site"](#).
- L'ajout d'un nouveau site n'augmente pas automatiquement le nombre d'objets que vous pouvez stocker. La capacité totale d'objets d'une grille dépend de l'espace de stockage disponible, de la politique ILM et de la capacité de métadonnées de chaque site.
- Lors du dimensionnement d'un nouveau site, vous devez vous assurer qu'il inclut suffisamment de capacité de métadonnées.

StorageGRID conserve une copie de toutes les métadonnées des objets sur chaque site. Lorsque vous ajoutez un nouveau site, assurez-vous qu'il dispose d'une capacité de métadonnées suffisante pour les métadonnées des objets existants et pour la croissance future.

Pour plus d'informations, veuillez consulter les documents suivants :

- ["Gérer le stockage des métadonnées d'objet"](#)
- ["Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage"](#)
- Vous devez tenir compte de la bande passante réseau disponible entre les sites et du niveau de latence du réseau. Les mises à jour des métadonnées sont continuellement répliquées entre les sites, même si tous les objets sont stockés uniquement sur le site où ils sont ingéré.

Pour éviter les mauvaises performances dues à la latence :

- Le codage par effacement n'est pas recommandé entre les sites présentant une latence supérieure à 100 ms.
- Les sites de votre système StorageGRID ne doivent pas s'étendre sur de grandes distances géographiques, par exemple, sur plusieurs continents.
- Votre système StorageGRID reste opérationnel pendant son développement. Vous devez donc revoir les règles ILM avant de démarrer la procédure d'extension. Vous devez vous assurer que les copies d'objet ne sont pas stockées sur le nouveau site tant que la procédure d'extension n'est pas terminée.

Par exemple, avant de commencer l'extension, vérifiez si des règles utilisent le pool de stockage par défaut (All Storage Nodes). Si c'est le cas, créez un nouveau pool de stockage avec les Storage Nodes existants et mettez à jour vos règles ILM pour utiliser le nouveau pool de stockage. Sinon, les objets sont copiés sur le nouveau site dès que le premier nœud de ce site devient actif.

Pour plus d'informations sur la modification d'une politique ILM lors de l'ajout d'un nouveau site, reportez-vous à la ["Exemple de modification d'une règle ILM"](#).

Préparez-vous à étendre votre système StorageGRID

Avant d'effectuer une opération d'extension, rassemblez les matériaux et installez et configurez tout nouveau matériel et tout nouveau réseau.

Élément	Remarques
Archive de l'installation de StorageGRID	Si vous ajoutez de nouveaux nœuds de grille ou un nouveau site, vous devez télécharger et extraire l'archive d'installation de StorageGRID. Vous devez utiliser la même version que celle actuellement en cours d'exécution sur la grille. Pour plus de détails, reportez-vous aux instructions Téléchargement et extraction des fichiers d'installation de StorageGRID de . Remarque : vous n'avez pas besoin de télécharger des fichiers si vous ajoutez de nouveaux volumes de stockage aux nœuds de stockage existants ou si vous installez une nouvelle appliance StorageGRID.
L'ordinateur portable de service	L'ordinateur portable de service présente les caractéristiques suivantes : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
Passwords.txt fichier	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le forfait de récupération.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement ne se trouve pas dans Passwords.txt le fichier.

Élément	Remarques
Documentation StorageGRID	• "Administrer StorageGRID" • "Notes de mise à jour". Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version. • "Instructions d'installation pour votre plate-forme"
Documentation actuelle pour votre plate-forme	Pour connaître les versions prises en charge, consultez le "Matrice d'interopérabilité (IMT)" .

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Avant de pouvoir ajouter de nouveaux nœuds de grille ou un nouveau site, vous devez télécharger l'archive d'installation StorageGRID appropriée et extraire les fichiers.

Description de la tâche

Vous devez effectuer des opérations d'extension à l'aide de la version de StorageGRID actuellement exécutée sur la grille.

Étapes

1. Allez à ["Téléchargement NetApp : StorageGRID"](#).
2. Sélectionnez la version de StorageGRID en cours d'exécution sur la grille.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
5. Dans la colonne **Install StorageGRID** de la page de téléchargement, sélectionnez le `.tgz` fichier ou `.zip` pour votre plate-forme.

La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installé.

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

Plateforme	Archive d'installation
RHEL	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

Plateforme	Archive d'installation
OpenStack/autre hyperviseur	Pour étendre un déploiement existant sur OpenStack, vous devez déployer une machine virtuelle exécutant l'une des distributions Linux prises en charge répertoriées ci-dessus et suivre les instructions appropriées pour Linux.

6. Téléchargez et extrayez le fichier d'archive.
7. Suivez les étapes appropriées pour votre plate-forme afin de choisir les fichiers dont vous avez besoin, en fonction de votre plate-forme, de la topologie de grille planifiée et de la manière dont vous allez étendre votre système StorageGRID.

Les chemins répertoriés dans l'étape pour chaque plate-forme sont relatifs au répertoire de niveau supérieur installé par le fichier d'archive.

8. Si vous étendez un système RHEL, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Progiciel RPM pour l'installation des images de nœud StorageGRID sur vos hôtes RHEL.
	Progiciel RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle Ansible et de manuel de vente pour la configuration des hôtes RHEL pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système Ubuntu ou Debian, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .

Chemin d'accès et nom de fichier	Description
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système VMware, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Le fichier modèle Open Virtualization format (.ovf) et le fichier manifeste (.mf) pour le déploiement du nœud d'administration principal.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement de nœuds Admin non primaires.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de passerelle.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système basé sur l'appliance StorageGRID, sélectionnez les fichiers appropriés.



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 où vous effectuez la procédure de récupération.

Chemin d'accès et nom de fichier	Description
	DEB package pour l'installation des images de noeud StorageGRID sur vos appareils.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .

Vérification du matériel et de la mise en réseau

Avant de commencer l'extension de votre système StorageGRID, vérifiez les points suivants :

- Le matériel nécessaire pour prendre en charge les nouveaux nœuds grid ou le nouveau site a été installé et configuré.
- Tous les nouveaux nœuds disposent de chemins de communication bidirectionnels vers tous les nœuds

existants et nouveaux (exigence pour le réseau Grid). Vérifiez en particulier que les ports TCP suivants sont ouverts entre les nouveaux nœuds que vous ajoutez dans l'extension et le nœud d'administration principal :

- 1055
- 7443
- 8011
- 10342

Voir "[Communications internes sur les nœuds de la grille](#)".

- Le nœud d'administration principal peut communiquer avec tous les serveurs d'extension destinés à héberger le système StorageGRID.
- Si l'un des nouveaux nœuds possède une adresse IP de réseau Grid sur un sous-réseau qui n'a pas été utilisé auparavant, vous avez déjà "[ajout du nouveau sous-réseau](#)" accès à la liste de sous-réseau Grid Network. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et recommencer la procédure.
- Vous n'utilisez pas la traduction d'adresses réseau (NAT) sur le réseau de grille entre les nœuds de grille ou entre les sites StorageGRID. Lorsque vous utilisez des adresses IPv4 privées pour le réseau Grid, ces adresses doivent être directement routables à partir de chaque nœud de la grille sur chaque site. L'utilisation de la fonction NAT pour relier le réseau Grid sur un segment de réseau public n'est prise en charge que si vous utilisez une application de tunneling transparente pour tous les nœuds de la grille, ce qui signifie que les nœuds de la grille ne nécessitent aucune connaissance des adresses IP publiques.

Cette restriction NAT est spécifique aux nœuds de la grille et au réseau Grid. Si nécessaire, vous pouvez utiliser NAT entre des clients externes et des nœuds de grille, par exemple pour fournir une adresse IP publique pour un nœud de passerelle.

Ajout de nœuds grid ou d'un site

Résumé du processus d'ajout de nœuds de grille ou de nouveaux sites à StorageGRID

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 racine ou autorisation de maintenance](#)".
- Tous les nœuds existants de la grille sont opérationnels sur tous les sites.
- Toute procédure d'extension, de mise à niveau, de déclassement ou de restauration est terminée.



Vous ne pouvez pas démarrer une extension pendant qu'une autre procédure d'extension, de mise à niveau, de récupération ou de mise hors service active est en cours. Toutefois, si nécessaire, vous pouvez interrompre une procédure de mise hors service pour démarrer une extension.

Étapes

1. "[Mise à jour des sous-réseaux pour le réseau Grid](#)".

2. ["Déployez les nouveaux nœuds de grille"](#).
3. ["Effectuer l'extension"](#).

Ajoutez ou mettez à jour des sous-réseaux au réseau Grid pour l'extension dans StorageGRID.

Lorsque vous ajoutez des nœuds de grille ou un nouveau site dans une extension, vous devrez peut-être mettre à jour ou ajouter des sous-réseaux au réseau Grid.

StorageGRID conserve une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de la grille sur le réseau Grid (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site du système StorageGRID, ainsi que tous les sous-réseaux utilisés pour les serveurs NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle réseau Grid.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Les adresses réseau des sous-réseaux que vous souhaitez configurer sont définies, en notation CIDR.

Description de la tâche

Si l'un des nouveaux nœuds possède une adresse IP de réseau Grid sur un sous-réseau non utilisé auparavant, vous devez ajouter le nouveau sous-réseau à la liste de sous-réseaux du réseau Grid avant de démarrer l'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et recommencer la procédure.

N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le Grid Network, l'Admin Network ou le Client Network de n'importe quel nœud :

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau Grid, 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 le mot de passe 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 automatiquement configurés pour votre système StorageGRID.

Déployez de nouveaux nœuds de grille dans StorageGRID

Les étapes du déploiement de nouveaux nœuds de grille dans une extension sont les mêmes que celles utilisées lors de l'installation initiale de la grille. Vous devez déployer tous les nouveaux nœuds de la grille avant de pouvoir réaliser l'extension.

Lorsque vous développez une grille, les nœuds que vous ajoutez n'ont pas à correspondre aux types de nœuds existants. Vous pouvez ajouter des nœuds VMware, des nœuds basés sur des conteneurs Linux ou des nœuds d'appliance.

VMware : déployez les nœuds grid

Vous devez déployer une machine virtuelle dans VMware vSphere pour chaque nœud VMware que vous souhaitez ajouter à l'extension.

Étapes

1. ["Déployez le nouveau nœud en tant que machine virtuelle"](#) et le connecter à un ou plusieurs réseaux StorageGRID .

Lorsque vous déployez le nœud, vous pouvez remappage les ports de nœud ou augmenter les paramètres de processeur ou de mémoire.

2. Après avoir déployé tous les nouveaux nœuds VMware, ["effectuer la procédure d'extension"](#).

Linux : déployez des nœuds grid

Vous pouvez déployer des nœuds grid sur de nouveaux hôtes Linux ou sur des hôtes Linux existants. Si vous avez besoin d'hôtes Linux supplémentaires pour prendre en charge les exigences en matière de processeur, de RAM et de stockage des nœuds StorageGRID que vous souhaitez ajouter à votre grille, vous devez les préparer de la même manière que lorsque vous les avez installés pour la première fois. Vous déployez ensuite les nœuds d'extension de la même manière que vous avez déployé des nœuds grid lors de l'installation.

Avant de commencer

- Vous disposez des instructions d'installation de StorageGRID pour votre version de Linux et vous avez examiné les ["exigences matérielles et de stockage"](#) .
- Si vous prévoyez de déployer de nouveaux nœuds grid sur des hôtes existants, vous avez confirmé que les hôtes existants disposent de suffisamment de processeur, de mémoire RAM et de capacité de stockage pour les nœuds supplémentaires.
- Vous disposez d'un plan pour réduire les domaines d'échec. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un hôte physique unique.



Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte physique ou virtuel. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

- Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

Étapes

1. Si vous ajoutez de nouveaux hôtes, accédez aux instructions d'installation pour le déploiement des nœuds StorageGRID.

2. Pour déployer les nouveaux hôtes, suivez les instructions de préparation des hôtes.
3. Pour créer des fichiers de configuration de nœuds et valider la configuration StorageGRID, suivez les instructions de déploiement des nœuds grid.
4. Si vous ajoutez des nœuds à un nouvel hôte Linux, démarrez le service d'hôte StorageGRID.
5. Si vous ajoutez des nœuds à un hôte Linux existant, démarrez les nouveaux nœuds à l'aide de l'interface de ligne de commande du service hôte StorageGRID :`sudo storagegrid node start [<node name\>]`

Une fois que vous avez terminé

Après le déploiement de tous les nouveaux nœuds de grille, vous pouvez ["réalisation de l'extension"](#).

Appliances : déploiement de nœuds de stockage, de passerelle ou d'administration non primaires

Pour installer le logiciel StorageGRID sur un nœud d'appliance, utilisez le programme d'installation de l'appliance StorageGRID, qui est inclus sur l'appliance. Dans une extension, chaque appliance de stockage fonctionne comme un seul nœud de stockage, et chaque appliance de services fonctionne comme un seul nœud de passerelle ou un nœud d'administration non primaire. Tout appareil peut se connecter au réseau Grid, au réseau Admin et au réseau client.

Avant de commencer

- L'appliance a été installée dans un rack ou une armoire, connectée à vos réseaux et sous tension.
- Vous avez terminé les ["Configurer le matériel"](#) étapes.

La configuration du matériel de l'appliance comprend les étapes requises pour configurer les connexions StorageGRID (liaisons réseau et adresses IP), ainsi que les étapes facultatives pour activer le chiffrement de nœud, modifier le mode RAID et remaper les ports réseau.

- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.
- Le firmware du programme d'installation de l'appliance StorageGRID sur l'appliance de remplacement est compatible avec la version du logiciel StorageGRID actuellement exécutée sur votre grid. Si les versions ne sont pas compatibles, vous devez mettre à niveau le micrologiciel du programme d'installation de l'appliance StorageGRID.
- Vous avez un ordinateur portable de service avec un ["navigateur web pris en charge"](#).
- Vous connaissez l'une des adresses IP attribuées au contrôleur de calcul de l'appliance. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.

Description de la tâche

Le processus d'installation de StorageGRID sur un nœud d'appliance comprend les phases suivantes :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud d'appliance.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.

Pendant les tâches d'installation de l'appliance, l'installation s'interrompt. Pour reprendre l'installation, connectez-vous au Grid Manager, approuvez tous les nœuds de la grille et terminez le processus d'installation de StorageGRID.



Si vous devez déployer plusieurs nœuds d'appliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du `configure-sga.py` script d'installation de l'appliance.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

`https://Controller_IP:8443`

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section connexion **Primary Admin Node**, déterminez si vous devez spécifier l'adresse IP du 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, soit présent sur le même sous-réseau.

3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	a. Décochez la case Activer la découverte du nœud d'administration. b. Saisissez l'adresse IP manuellement. c. Sélectionnez Enregistrer. d. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case Activer la découverte du nœud d'administration. b. Attendez que la liste des adresses IP découvertes s'affiche. c. Sélectionnez le nœud d'administration principal de la grille dans laquelle ce nœud de stockage de l'appliance sera déployé. d. Sélectionnez Enregistrer. e. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.

4. Dans le champ **Nom du nœud**, entrez le nom que vous souhaitez utiliser pour ce nœud de l'appliance, puis sélectionnez **Enregistrer**.

Le nom de nœud est attribué à ce nœud d'appliance dans le système StorageGRID. Elle s'affiche sur la page nœuds (onglet Présentation) dans Grid Manager. Si nécessaire, vous pouvez modifier le nom du nœud lors de l'approbation.

5. Dans la section **installation**, vérifiez que l'état actuel est "prêt à démarrer l'installation de *nom de nœud* dans la grille avec le nœud Admin principal *admin_ip*" et que le bouton **Démarrer l'installation** est activé.

Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou

les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

6. Dans la page d'accueil du programme d'installation de l'apppliance StorageGRID, sélectionnez **Démarrer l'installation**.

L'état actuel passe à « Installation en cours », et la page d'installation du moniteur s'affiche.

7. Si votre extension inclut plusieurs nœuds d'apppliance, répétez les étapes précédentes pour chaque appliance.



Si vous devez déployer plusieurs nœuds de stockage d'apppliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du script d'installation de l'apppliance `configure-sga.py`.

8. Si vous devez accéder manuellement à la page d'installation du moniteur, sélectionnez **Installation du moniteur** dans la barre de menu.

La page d'installation de Monitor affiche la progression de l'installation.

La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.



Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état « ignoré ».

9. Passez en revue l'état d'avancement des deux premières étapes d'installation.

1. Configurer l'apppliance

Au cours de cette étape, l'un des processus suivants se produit :

- Pour une appliance de stockage, le programme d'installation se connecte au contrôleur de stockage, efface toute configuration existante, communique avec SANtricity OS pour configurer les volumes et configure les paramètres de l'hôte.
- Pour une appliance de services, le programme d'installation efface toute configuration existante des disques du contrôleur de calcul et configure les paramètres de l'hôte.

2. Installez OS

Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'apppliance.

10. Continuez à surveiller la progression de l'installation jusqu'à ce qu'un message s'affiche dans la fenêtre de la console, vous invitant à utiliser le gestionnaire de grille pour approuver le nœud.



Attendez que tous les nœuds ajoutés à cette extension soient prêts pour approbation avant de passer à Grid Manager pour approuver les nœuds.

Effectuez une extension StorageGRID

Lorsque vous effectuez l'extension, des nœuds grid sont ajoutés à votre déploiement StorageGRID existant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé tous les nœuds grid qui sont ajoutés dans cette extension.
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Si vous ajoutez des nœuds de stockage, vous avez confirmé que toutes les opérations de réparation de données réalisées dans le cadre d'une restauration sont terminées. Voir ["Vérifier les travaux de réparation des données"](#).
- Si vous ajoutez des nœuds de stockage et que vous souhaitez attribuer un niveau de stockage personnalisé à ces nœuds, vous avez déjà ["création du niveau de stockage personnalisé"](#). Vous disposez également de l'autorisation d'accès racine ou des autorisations Maintenance et ILM.
- Si vous ajoutez un nouveau site, vous avez examiné et mis à jour les règles ILM. Vous devez vous assurer que les copies d'objet ne sont pas stockées sur le nouveau site tant que l'extension n'est pas terminée. Par exemple, si une règle utilise le pool de stockage par défaut (**tous les nœuds de stockage**), vous devez ["créer un nouveau pool de stockage"](#) qui contient uniquement les nœuds de stockage existants et ["Mise à jour des règles ILM"](#) la stratégie ILM pour utiliser ce nouveau pool de stockage. Sinon, les objets seront copiés sur le nouveau site dès que le premier nœud de ce site devient actif.

Description de la tâche

L'exécution de l'extension inclut les tâches utilisateur principales suivantes :

1. Configurer l'extension.
2. Démarrez l'extension.
3. Téléchargez un nouveau fichier de package de récupération.
4. Surveillez les étapes et étapes d'extension jusqu'à ce que tous les nouveaux nœuds soient installés et configurés et que tous les services aient démarré.



L'exécution de certaines étapes et étapes d'extension sur un grand grid peut prendre beaucoup de temps. Par exemple, si la base de données Cassandra est vide, vous pouvez streamer Cassandra vers un nouveau nœud de stockage. Cependant, si la base de données Cassandra inclut un volume important de métadonnées d'objet, cette étape peut prendre plusieurs heures, voire plus. Ne redémarrez aucun nœud de stockage pendant les étapes « extension du cluster Cassandra » ou « démarrage de Cassandra et des données de streaming ».

Étapes

1. Sélectionnez **Maintenance > Tâches > Grid expansion**.

La page d'extension de la grille s'affiche. La section Nœuds en attente liste les nœuds prêts à être ajoutés.

2. Sélectionnez **configurer l'extension**.

La boîte de dialogue sélection du site s'affiche.

3. Sélectionnez le type d'expansion que vous commencez :
 - Si vous ajoutez un nouveau site, sélectionnez **Nouveau** et entrez le nom du nouveau site.
 - Si vous ajoutez un ou plusieurs nœuds à un site existant, sélectionnez **existant**.
4. Sélectionnez **Enregistrer**.
5. Consultez la liste **nœuds en attente** et vérifiez qu'elle affiche tous les nœuds de la grille que vous avez déployés.

Si nécessaire, vous pouvez placer votre curseur sur l'adresse **Grid Network MAC Address** d'un nœud pour afficher les détails sur ce nœud.

The screenshot shows a web interface titled "Pending Nodes". On the left, there is a list of nodes with radio buttons for selection. The first node has a MAC address of 00:50:56:a7:7a:c0. Below this list is a section for "Approved Nodes". On the right, a detailed view of a selected node is shown. The node is named "rleo-010-096-106-151" and is a "Storage Node". It lists network information: Grid Network (10.96.106.151/22), Admin Network (10.96.104.1), and Client Network. Hardware details include VMware VM, 4 CPUs, and 8 GB RAM. Disk details show three 55 GB disks.



Si un nœud est manquant, vérifiez qu'il a été déployé avec succès.

6. Dans la liste des nœuds en attente, approuvez les nœuds que vous souhaitez ajouter à cette extension.
 - a. Sélectionnez le bouton radio à côté du premier nœud de grille en attente que vous souhaitez approuver.
 - b. Sélectionnez **approuver**.

Le formulaire de configuration des nœuds de la grille s'affiche.

- c. Si nécessaire, modifiez les paramètres généraux :

Champ	Description
Le site	Nom du site auquel le nœud de grille sera associé. Si vous ajoutez plusieurs nœuds, veillez à sélectionner le site approprié pour chaque nœud. Si vous ajoutez un site, tous les nœuds sont ajoutés au nouveau site.

Champ	Description
Nom	Nom du système du 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 des métadonnées et des données 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 (pas de données d'objet)
Rôle NTP	Le rôle NTP (Network Time Protocol) du nœud de grille : • Sélectionnez automatique (par défaut) pour attribuer automatiquement le rôle NTP au nœud. Le rôle principal sera attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille ayant des adresses IP non statiques. Le rôle client sera attribué à tous les autres nœuds de la grille. • Sélectionnez principal pour attribuer manuellement le rôle NTP principal au nœud. Au moins deux nœuds sur chaque site doivent avoir le rôle principal pour fournir un accès système redondant aux sources de synchronisation externes. • Sélectionnez client pour attribuer manuellement le rôle NTP du client au nœud.
Service ADC (nœuds de stockage combinés ou 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. • Sélectionnez Oui si le nœud de stockage que vous remplacez inclut le service ADC. Étant donné que vous ne pouvez pas désactiver un nœud de stockage s'il reste trop peu de services ADC, ce paramètre garantit qu'un nouveau service ADC est disponible avant la suppression de l'ancien service. • Tu peux "déplacer le service ADC vers un autre nœud de stockage sur le même site" pour garantir que le quorum du service ADC soit respecté. • Sélectionnez automatique pour permettre au système de déterminer si ce nœud nécessite le service ADC. En savoir plus sur "Quorum ADC"le .

Champ	Description
Niveau de stockage (nœuds de stockage combinés ou uniquement des données)	Utilisez le niveau de stockage par défaut ou sélectionnez le niveau de stockage personnalisé que vous souhaitez affecter à ce nouveau nœud. Les niveaux de stockage sont utilisés par les pools de stockage ILM. Ainsi, votre sélection peut affecter les objets qui seront placés sur le nœud de stockage.

d. Si nécessaire, modifiez les paramètres du réseau Grid, du réseau Admin et du réseau client.

- **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface réseau. Par exemple : 172.16.10.100/24



Si vous découvrez que les nœuds ont des adresses IP dupliquées sur le réseau Grid alors que vous approuvez des nœuds, vous devez annuler l'extension, redéployer les machines virtuelles ou les appliances avec une adresse IP non dupliquée, puis redémarrer l'extension.

- **Gateway** : passerelle par défaut du nœud de la grille. Par exemple : 172.16.10.1
- **Sous-réseaux (CIDR)** : un ou plusieurs sous-réseaux pour le réseau Admin.

e. Sélectionnez **Enregistrer**.

Le nœud de grille approuvé passe à la liste nœuds approuvés.

- Pour modifier les propriétés d'un nœud de grille approuvé, sélectionnez son bouton radio et sélectionnez **Modifier**.
- Pour déplacer un nœud de grille approuvé vers la liste nœuds en attente, sélectionnez son bouton d'option et sélectionnez **Réinitialiser**.
- Pour supprimer définitivement un nœud de grille approuvé, mettez le nœud hors tension. Ensuite, sélectionnez son bouton radio et sélectionnez **Supprimer**.

f. Répétez ces étapes pour chaque nœud de grille en attente à approuver.



Si possible, vous devez approuver toutes les notes de grille en attente et effectuer une extension unique. Plus de temps sera nécessaire si vous réalisez plusieurs petits expansions.

7. Une fois que vous avez approuvé tous les nœuds de la grille, saisissez la **phrase secrète de provisionnement** et sélectionnez **Expand**.

Au bout de quelques minutes, cette page se met à jour pour afficher l'état de la procédure d'extension. Lorsque des tâches qui affectent des nœuds de grille individuels sont en cours, la section Etat du nœud de grille répertorie l'état actuel de chaque nœud de grille.



Lors de l'étape « installation de nœuds de grille » pour une nouvelle appliance, le programme d'installation de l'appliance StorageGRID indique que l'installation passe de l'étape 3 à l'étape 4, finalisation de l'installation. Une fois l'étape 4 terminée, le contrôleur est redémarré.



L'extension de site inclut une tâche supplémentaire pour configurer Cassandra pour le nouveau site.

8. Dès que le lien **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 de package de récupération vous permet de restaurer le système en cas de panne.

- a. Sélectionnez le lien de téléchargement.
- b. Saisissez le mot de passe de provisionnement et sélectionnez **Démarrer le téléchargement**.
- c. Une fois le téléchargement terminé, ouvrez `.zip` le fichier et confirmez que vous pouvez accéder au contenu, y compris au `Passwords.txt` fichier.
- d. 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 du système StorageGRID .

9. Si vous ajoutez des nœuds de stockage à un site existant ou que vous ajoutez un site, surveillez les étapes Cassandra qui se produisent lorsque les services sont démarrés sur les nouveaux nœuds de grille.



Ne redémarrez aucun nœud de stockage pendant les étapes « extension du cluster Cassandra » ou « démarrage de Cassandra et des données de streaming ». Ces étapes peuvent prendre plusieurs heures pour chaque nouveau nœud de stockage, en particulier si les nœuds de stockage existants contiennent une quantité importante de métadonnées d'objet.

Ajout de nœuds de stockage

Si vous ajoutez des nœuds de stockage à un site existant, consultez le pourcentage affiché dans le message d'état « démarrage de Cassandra et données en streaming ».

Ce pourcentage estime que le streaming Cassandra est complet, en fonction du volume total de données Cassandra disponibles et du volume qui a déjà été écrit sur le nouveau nœud.

Ajout d'un site

Si vous ajoutez un nouveau site, utilisez `nodetool status` pour surveiller la progression du streaming Cassandra et pour voir la quantité de métadonnées copiées sur le nouveau site lors de l'étape d'extension du cluster Cassandra. La charge totale des données sur le nouveau site devrait se situer à environ 20 % du total d'un site actuel.

10. Continuez à surveiller l'extension jusqu'à ce que toutes les tâches soient terminées et que le bouton **Configure expansion** réapparaisse.

Une fois que vous avez terminé

En fonction des types de nœuds de grille que vous avez ajoutés, effectuez des étapes supplémentaires d'intégration et de configuration. Voir "[Étapes de configuration après l'extension](#)".

Ajout de volumes de stockage

Ajoutez des volumes de stockage à votre système StorageGRID

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, "[instructions d'ajout de capacité d'objet](#)" vérifiez que vous savez où ajouter des volumes afin de répondre aux exigences de votre règle ILM.



Ces instructions s'appliquent uniquement aux nœuds de stockage basés sur logiciel. Voir "[Ajout du tiroir d'extension au SG6060 déployé](#)" ou "[Ajout du tiroir d'extension au SG6160 déployé](#)" pour apprendre à ajouter des volumes de stockage aux SG6060 ou SG6160 en installant des tiroirs d'extension. Les autres nœuds de stockage de l'apppliance ne peuvent pas être étendus.

Description de la tâche

Le stockage sous-jacent d'un nœud de stockage est divisé en volumes de stockage. Les volumes de stockage sont des périphériques de stockage basés sur des blocs formatés par le système StorageGRID et montés pour stocker des objets. Chaque nœud de stockage peut prendre en charge jusqu'à 48 volumes de stockage, appelés *object stores* dans Grid Manager.



Les métadonnées d'objet sont toujours stockées dans le magasin d'objets 0.

Chaque magasin d'objets est monté sur un volume qui correspond à son ID. Par exemple, le magasin d'objets avec un ID de 0000 correspond au `/var/local/rangedb/0` point de montage.

Avant d'ajouter de nouveaux volumes de stockage, utilisez la grille Manager pour afficher les magasins d'objets actuels pour chaque nœud de stockage ainsi que les points de montage correspondants. Vous pouvez utiliser ces informations lors de l'ajout de volumes de stockage.

Étapes

1. Sélectionnez **Nœuds** > **site** > **Nœud de stockage** > **Stockage**.
2. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

Pour les nœuds de stockage de l'apppliance, le nom mondial de chaque disque correspond à l'identifiant WWID (WWID) du volume qui s'affiche lorsque vous affichez les propriétés standard du volume dans SANtricity OS (le logiciel de gestion connecté au contrôleur de stockage de l'apppliance).

Pour vous aider à interpréter les statistiques de lecture et d'écriture du disque relatives aux points de montage du volume, la première partie du nom affichée dans la colonne **Name** de la table Disk Devices (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur indiquée dans la colonne **Device** de la table volumes.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. Suivez les instructions fournies par votre plateforme pour ajouter de nouveaux volumes de stockage au nœud de stockage.
 - ["VMware : ajoutez des volumes de stockage au nœud de stockage"](#)
 - ["Linux : ajoutez des volumes SAN ou DAS au nœud de stockage"](#)

Ajoutez des volumes de stockage aux nœuds de stockage VMware dans StorageGRID

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 à la ["instructions d'installation de StorageGRID pour les déploiements VMware"](#).
- Vous avez le `Passwords.txt` fichier.
- Vous avez ["autorisations d'accès spécifiques"](#).



N'essayez pas d'ajouter des volumes de stockage à un nœud de stockage pendant qu'une mise à niveau logicielle, une procédure de restauration ou une autre procédure d'extension est active.

Description de la tâche

Le nœud de stockage n'est pas disponible brièvement lorsque vous ajoutez des volumes de stockage. Cette procédure doit être effectuée sur un seul nœud de stockage à la fois pour éviter d'affecter les services de grid côté client.

Étapes

1. Si nécessaire, installez un nouveau matériel de stockage et créez de nouveaux datastores VMware.
2. Ajoutez un ou plusieurs disques durs à la machine virtuelle pour l'utiliser comme stockage (magasins d'objets).

- a. Ouvrez le client VMware vSphere.
- b. Modifiez les paramètres de la machine virtuelle pour ajouter un ou plusieurs disques durs supplémentaires.

Les disques durs sont généralement configurés en tant que disques d'ordinateurs virtuels (VMDK, Virtual machine Disks). Les VMDK sont plus fréquemment utilisés et plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo). Pour plus d'informations sur l'ajout de disques durs aux machines virtuelles, consultez la documentation de VMware vSphere.

3. Redémarrez la machine virtuelle à l'aide de l'option **redémarrer le système d'exploitation invité** du 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. Configurez le nouveau stockage pour qu'il soit utilisé par le nœud de stockage :
 - a. Connectez-vous au nœud grid :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`

- ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- iii. Entrez la commande suivante pour basculer en root : `su -`
- iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Configurer les nouveaux volumes de stockage :

```
sudo add_rangedbs.rb
```

Ce script trouve tous les nouveaux volumes de stockage et vous invite à les formater.

- c. Saisissez **y** pour accepter le formatage.
- d. Si l'un des volumes a déjà été formaté, décidez si vous souhaitez les reformater.
 - Entrez **y** pour reformater.
 - Saisissez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` script s'exécute automatiquement.

5. Vérifier que les services démarrent correctement :

- a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

L'état est mis à jour automatiquement.

- a. Attendez que tous les services soient en cours d'exécution ou vérifiés.
- b. Quitter l'écran d'état :

```
Ctrl+C
```

6. Vérifiez que le nœud de stockage est en ligne :

- a. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- b. Sélectionnez **Nœuds > Nœud de stockage > Tâches**.
- c. Si la liste déroulante **État de stockage** est définie sur Lecture seule ou Hors ligne, sélectionnez **En ligne**.
- d. Sélectionnez **Enregistrer**.

7. Pour voir les nouveaux magasins d'objets, sélectionnez **Stockage**.

8. Consultez les détails dans le tableau **Volumes**.

Résultat

Vous pouvez utiliser la capacité étendue des nœuds de stockage pour sauvegarder les données d'objet.

Ajoutez des volumes à connexion directe ou SAN aux nœuds de stockage Linux dans StorageGRID

Si un nœud de stockage contient moins de 48 volumes de stockage, vous pouvez augmenter sa capacité en ajoutant de nouveaux périphériques de stockage en mode

bloc, en les rendant visibles pour les hôtes Linux et en ajoutant les nouveaux mappages de périphériques de bloc au fichier de configuration StorageGRID utilisé pour le nœud de stockage.

Avant de commencer

- Vous avez accès à la ["instructions pour l'installation de StorageGRID"](#) pour votre plateforme Linux.
- Vous avez le `Passwords.txt` fichier.
- Vous avez ["autorisations d'accès spécifiques"](#).



N'essayez pas d'ajouter des volumes de stockage à un nœud de stockage pendant qu'une mise à niveau logicielle, une procédure de restauration ou une autre procédure d'extension est active.

Description de la tâche

Le nœud de stockage n'est pas disponible brièvement lorsque vous ajoutez des volumes de stockage. Cette procédure doit être effectuée sur un seul nœud de stockage à la fois pour éviter d'affecter les services de grid côté client.

Étapes

1. Installez le nouveau matériel de stockage.

Pour plus d'informations, consultez la documentation fournie par votre fournisseur de matériel.

2. Créer de nouveaux volumes de stockage en mode bloc de la taille souhaitée.
 - Connectez les nouveaux disques et mettez à jour la configuration du contrôleur RAID si nécessaire, ou allouez les nouvelles LUN SAN sur les baies de stockage partagées et autorisez l'hôte Linux à y accéder.
 - Utilisez le même schéma de nommage persistant que celui utilisé pour les volumes de stockage sur le nœud de stockage existant.
 - Si vous utilisez la fonctionnalité de migration de nœud StorageGRID, rendez les nouveaux volumes visibles pour les autres hôtes Linux qui sont des cibles de migration pour ce nœud de stockage. Pour plus d'informations, reportez-vous aux instructions d'installation de StorageGRID pour votre plateforme Linux.
3. Connectez-vous à l'hôte Linux prenant en charge le nœud de stockage en tant qu'utilisateur root ou à l'aide d'un compte disposant de l'autorisation sudo.
4. Vérifiez que les nouveaux volumes de stockage sont visibles sur l'hôte Linux.

Il se peut que vous deviez effectuer une nouvelle analyse pour les périphériques.

5. Exécutez la commande suivante pour désactiver temporairement le nœud de stockage :

```
sudo storagegrid node stop <node-name>
```

6. A 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 de nœud contenant les mappages de périphériques de bloc de stockage objet existants.

Dans l'exemple, `BLOCK_DEVICE_RANGEDB_00` à `BLOCK_DEVICE_RANGEDB_03` correspondent aux mappages de périphériques de bloc de stockage objet existants.

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

8. Ajoutez de nouveaux mappages de périphériques de blocs de stockage objet correspondant aux volumes de stockage bloc que vous avez ajoutés pour ce nœud de stockage.

Assurez-vous de commencer à la prochaine BLOCK_DEVICE_RANGEDB_nn. Ne laissez pas de place.

- Sur la base de l'exemple ci-dessus, commencez à BLOCK_DEVICE_RANGEDB_04.
- Dans l'exemple ci-dessous, quatre nouveaux volumes de stockage en mode bloc ont été ajoutés au nœud : BLOCK_DEVICE_RANGEDB_04 à BLOCK_DEVICE_RANGEDB_07.

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

9. Exécutez la commande suivante pour valider les modifications apportées au fichier de configuration de nœud pour le nœud de stockage :

```
sudo storagegrid node validate <node-name>
```

Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

Si vous observez une erreur similaire à ce qui suit, cela signifie que le fichier de configuration de nœud tente de mapper le périphérique de bloc utilisé par <node-name> pour <PURPOSE> à donné <path-name> dans le système de fichiers Linux, mais qu'il n'existe pas de fichier spécial de périphérique de bloc valide (ou de lien logiciel vers un fichier spécial de périphérique de bloc) à cet emplacement.



```
Checking configuration file for node <node-name>...  
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>  
<path-name> is not a valid block device
```

Vérifiez que vous avez saisi le bon <path-name>.

10. Exécutez la commande suivante pour redémarrer le nœud avec les nouveaux mappages de périphériques de bloc en place :

```
sudo storagegrid node start <node-name>
```

11. Connectez-vous au nœud de stockage en tant qu'administrateur à l'aide du mot de passe indiqué dans Passwords.txt le fichier.

12. Vérifier que les services démarrent correctement :

- a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

L'état est mis à jour automatiquement.

- b. Attendez que tous les services soient en cours d'exécution ou vérifiés.

- c. Quitter l'écran d'état :

```
Ctrl+C
```

13. Configurez le nouveau stockage pour qu'il soit utilisé par le nœud de stockage :

- a. Configurer les nouveaux volumes de stockage :

```
sudo add_rangedbs.rb
```

Ce script trouve tous les nouveaux volumes de stockage et vous invite à les formater.

- b. Entrez **y** pour formater les volumes de stockage.

- c. Si l'un des volumes a déjà été formaté, décidez si vous souhaitez les reformater.

- Entrez **y** pour reformater.
- Saisissez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` script s'exécute automatiquement.

14. Vérifiez que l'état du stockage du nœud de stockage est en ligne :

- a. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- b. Sélectionnez **Nœuds > Nœud de stockage > Tâches**.
- c. Si la liste déroulante **État de stockage** est définie sur Lecture seule ou Hors ligne, sélectionnez **En ligne**.
- d. Sélectionnez **Enregistrer**.

15. Pour voir les nouveaux magasins d'objets, sélectionnez **Stockage**.

16. Consultez les détails dans le tableau **Volumes**.

Résultat

Vous pouvez maintenant utiliser la capacité étendue des nœuds de stockage pour sauvegarder les données d'objet.

Configuration du système faisant l'objet de l'extension

Configurez les nœuds et sites nouvellement ajoutés dans StorageGRID.

Une fois l'extension terminée, vous devez effectuer d'autres étapes d'intégration et de configuration.

Description de la tâche

Vous devez effectuer les tâches de configuration répertoriées ci-dessous pour les nœuds grid ou les sites que vous ajoutez à votre extension. Certaines tâches peuvent être facultatives, selon les options sélectionnées lors de l'installation et de l'administration du système, et selon la façon dont vous souhaitez configurer les nœuds et les sites ajoutés au cours de l'extension.

Étapes

1. Si vous avez ajouté un site :
 - ["Créer un pool de stockage"](#) Pour le site et chaque niveau de stockage que vous avez sélectionnés pour les nouveaux nœuds de stockage.
 - Vérification de la conformité de la politique ILM aux nouvelles exigences Si des modifications de règle sont requises, ["créer de nouvelles règles"](#) et ["Mise à jour de la règle ILM"](#). Si les règles sont déjà correctes, ["activer une nouvelle stratégie"](#) sans modification de règle pour garantir que StorageGRID utilise les nouveaux nœuds.
 - Vérifiez que les serveurs NTP (Network Time Protocol) sont accessibles depuis ce site. Voir ["Gérer les serveurs NTP"](#).



Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

2. Si vous avez ajouté un ou plusieurs nœuds de stockage à un site existant :
 - ["Afficher les détails du pool de stockage"](#) Vous pouvez vérifier que chaque nœud ajouté est inclus dans les pools de stockage attendus et utilisé dans les règles ILM attendues.
 - Vérification de la conformité de la politique ILM aux nouvelles exigences Si des modifications de règle sont requises, ["créer de nouvelles règles"](#) et ["Mise à jour de la règle ILM"](#). Si les règles sont déjà

correctes, "[activer une nouvelle stratégie](#)" sans 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 avec code d'effacement. Voir "[Rééquilibrent les données codées après l'ajout de nœuds de stockage](#)".

3. Si vous avez ajouté un nœud de passerelle :

- Si des groupes 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 "[Configurez les groupes 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 à ce nœud tant que vous n'avez pas créé cette approbation de partie de confiance. Reportez-vous à la configuration de l'authentification unique (SSO) à l'aide de "[OIDC](#)" ou "[SAML](#)".
- 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 "[Configurez les groupes haute disponibilité](#)".
- c. Si vous souhaitez conserver la cohérence des metrics historiques sur chaque nœud d'administration, vous pouvez également copier la base de données Prometheus du nœud d'administration principal vers le nœud d'administration d'extension. Voir "[Copie des metrics Prometheus](#)".
- d. Si vous souhaitez conserver la cohérence des informations du journal historique sur chaque nœud d'administration, copiez les journaux d'audit existants du nœud d'administration principal vers le nœud d'administration d'extension. Voir "[Copie des journaux d'audit](#)".

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 fiable, les connexions au nœud sur le réseau client doivent être effectuées à l'aide d'un nœud final d'équilibreur de charge. Voir "[Configurer les terminaux de l'équilibreur de charge](#)" et "[Gérer les contrôles de pare-feu](#)".

6. Configurez le DNS.

Si vous avez spécifié des paramètres DNS séparément pour chaque nœud de grid, vous devez ajouter des paramètres DNS personnalisés par nœud pour les nouveaux nœuds. Voir "[Modifiez la configuration DNS pour un nœud de grid unique](#)".

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

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Vérifiez que les nœuds de stockage sont actifs après une extension de StorageGRID

Une fois une opération d'extension qui ajoute de nouveaux nœuds de stockage terminée, le système StorageGRID doit démarrer automatiquement à l'aide des nouveaux nœuds de stockage. Vous devez utiliser le système StorageGRID pour vérifier que le nouveau nœud de stockage est actif.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Sélectionnez **Nœuds > Nœud de stockage d'extension > Stockage**.
3. Placez votre curseur sur le graphique **stockage utilisé - données d'objet** pour afficher la valeur de **utilisé**, qui est la quantité d'espace utilisable total utilisée pour les données d'objet.
4. Vérifiez que la valeur de **utilisé** augmente au fur et à mesure que vous déplacez le curseur vers la droite du graphique.

Copiez les métriques Prometheus vers les nouveaux nœuds d'administration dans StorageGRID.

Après avoir ajouté un nouveau nœud d'administration, vous pouvez éventuellement copier les metrics historiques gérés par Prometheus du nœud d'administration principal vers le nouveau nœud d'administration. La copie des metrics garantit la cohérence des mesures historiques entre les nœuds d'administration.

Avant de commencer

- Le nouveau nœud d'administration est installé et en cours d'exécution.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Lorsque vous ajoutez un nœud d'administration, le processus d'installation logicielle crée une nouvelle base de données Prometheus. Vous pouvez conserver la cohérence des metrics historiques entre les nœuds en copiant la base de données Prometheus du nœud d'administration principal (*source Admin Node*) vers le nouveau nœud d'administration.



La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`

3. Suivez les étapes suivantes sur le nouveau nœud d'administration :

a. Connectez-vous au nouveau nœud d'administration :

i. Entrez la commande suivante : `ssh admin@grid_node_IP`

ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour basculer en root : `su -`

iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

b. Arrêtez le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

d. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nouveau nœud d'administration : `/usr/local/prometheus/bin/prometheus-clone-db.sh`
`Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nouveau 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. L'état suivant apparaît :

```
Database cloned, starting services
```

a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :

```
ssh-add -D
```

4. Redémarrez le service Prometheus sur le nœud d'administration source.

```
service prometheus start
```

Copiez les journaux d'audit vers les nouveaux nœuds d'administration dans StorageGRID.

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` fichier.

Description de la tâche

Pour rendre disponibles les messages d'audit historiques sur un nouveau nœud d'administration, vous devez copier manuellement les fichiers journaux d'audit d'un nœud d'administration existant vers le nœud d'administration d'extension.



Par défaut, les informations d'audit sont envoyées à l' `localaudit` connectez-vous sur chaque nœud. Pour utiliser cette procédure, vous devez avoir configuré les nœuds d'administration comme destination d'audit comme suit :

- Vous avez configuré **Nœuds d'administration/nœuds locaux** comme destination du journal.
- Vous avez configuré **Nœuds d'administration et serveur syslog externe** comme destination du journal.

Se référer à "[Configurer les messages d'audit et le serveur syslog externe](#)" 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier : `service ams stop`

3. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/audit/export/
```

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 du nœud d'administration d'extension :

```
scp -p * IP_address:/var/local/audit/export/
```

6. Si vous êtes invité à saisir la phrase de passe pour `/root/.ssh/id_rsa`, entrez le mot de passe d'accès SSH du nœud d'administration principal répertorié dans `Passwords.txt` le fichier.

7. Restaurez le fichier d'origine `audit.log` :

```
mv new_name.txt audit.log
```

8. Démarrez le service AMS :

```
service ams start
```

9. Déconnexion du serveur :

```
exit
```

10. Connectez-vous au nœud d'administration d'extension :

- Entrez la commande suivante : `ssh admin@expansion_Admin_Node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

11. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit :

```
cd /var/local/audit/export/  
  
chown ams-user:bycast *
```

12. Déconnexion du serveur :

```
exit
```

Rééquilibrez les données à codage d'effacement après l'ajout de nœuds à votre système StorageGRID.

Après avoir ajouté des nœuds de stockage, vous pouvez utiliser la procédure de rééquilibrage du code d'effacement pour redistribuer les fragments avec code d'effacement entre les nœuds de stockage existants et les nouveaux nœuds.

Avant de commencer

- Vous avez terminé les étapes d'extension pour ajouter les nouveaux nœuds de stockage.
- Vous avez examiné le ["considérations relatives au rééquilibrage des données avec code d'effacement"](#).
- Vous comprenez que les données d'objet répliquées ne seront pas déplacées par cette procédure et que la procédure de rééquilibrage EC ne déplace pas les données répliquées. Cependant, les données répliquées sont prises en compte pour déterminer où déplacer les données EC.
- Vous avez le `Passwords.txt` fichier.

Que se passe-t-il lorsque cette procédure est exécutée

Avant de commencer la procédure, noter les points suivants :

- La procédure de rééquilibrage EC ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.
- La procédure de rééquilibrage EC réserve temporairement une grande quantité de stockage. Les alertes de stockage peuvent être déclenchées, mais elles seront résolues une fois le rééquilibrage terminé. S'il n'y

a pas assez de stockage pour la réservation, la procédure de rééquilibrage EC échoue. Les réservations de stockage sont libérées lorsque la procédure de rééquilibrage EC est terminée, que la procédure ait échoué ou a réussi.

- Si un volume passe hors ligne alors que la procédure de rééquilibrage EC est en cours, la procédure de rééquilibrage prend fin. Tout fragment de données déjà déplacé restera dans son nouvel emplacement, et aucune donnée ne sera perdue.

Vous pouvez relancer la procédure une fois que tous les volumes sont de nouveau en ligne.

- L'exécution de la procédure de rééquilibrage EC peut avoir un impact sur les performances des opérations ILM et des opérations client S3.



Les opérations de l'API S3 pour le téléchargement d'objets (ou de parties d'objets) peuvent échouer lors de la procédure de rééquilibrage de l'EC s'ils nécessitent plus de 24 heures. Les opérations PUT de longue durée échouent si la règle ILM applicable utilise un placement équilibré ou strict à l'entrée. L'erreur suivante sera signalée : 500 Internal Server Error.

- **Conditions d'achèvement du travail.** La procédure de rééquilibrage EC est considérée comme terminée lorsque l'une des conditions suivantes est vraie :
 - Elle ne peut plus déplacer de données avec code d'effacement.
 - Les données de tous les nœuds présentent un écart de 5 % maximum par rapport à la partition d'espace utilisable cible.
 - La procédure est en cours d'exécution depuis 30 jours.

Étapes

1. consultez les détails actuels du stockage objet pour le site que vous prévoyez de rééquilibrer.
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez le premier nœud de stockage du site.
 - c. Sélectionnez l'onglet **stockage**.
 - d. Positionnez le curseur de votre souris sur le graphique stockage utilisé - données d'objet pour afficher la quantité actuelle de données répliquées et de données avec code d'effacement sur le nœud de stockage.
 - e. Répétez cette procédure pour afficher les autres nœuds de stockage du site.
2. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Démarrer la procédure :

``démarrage de la solution reallbalance-data --site "site-name"`

Pour "site-name", spécifiez le premier site où vous avez ajouté un ou plusieurs nœuds de stockage.

Placez-les `site-name` entre guillemets.

La procédure de rééquilibrage EC démarre et un ID de tâche est renvoyé.

4. Copier l'ID du travail.

5. surveiller l'état de la procédure de rééquilibrage EC.

- Pour afficher le statut d'une procédure de rééquilibrage EC unique :

```
rebalance-data status --job-id job-id
```

Pour *job-id*, spécifiez l'ID qui a été renvoyé lorsque vous avez démarré la procédure.

- Pour afficher le statut de la procédure de rééquilibrage EC actuelle et toutes les procédures précédemment effectuées :

```
rebalance-data status
```



Pour obtenir de l'aide sur la commande rééquilibrer-données :

```
rebalance-data --help
```

6. Effectuer des étapes supplémentaires en fonction de l'état renvoyé :

- Si `State` est `In progress`, l'opération de rééquilibrage EC est toujours en cours d'exécution. Vous devez régulièrement surveiller la procédure jusqu'à ce qu'elle soit terminée.

Accédez à la page [Nœuds](#) pour évaluer la répartition des données sur les nœuds de stockage du site.

La tâche de rééquilibrage EC est considérée comme terminée et s'arrêtera lorsque l'espace utilisable dans tous les nœuds sera à moins de 5 % de la partition d'espace utilisable cible.

- Si `State` est `Success`, facultatif [examinez le stockage objet](#) pour voir les détails mis à jour pour le site.

L'espace utilisable devrait désormais être mieux réparti entre les nœuds de stockage du site.

- Si `State` est `Failure` :

- i. Vérifiez que tous les nœuds de stockage du site sont connectés à la grille.
- ii. Recherchez et résolvez les alertes susceptibles d'affecter ces nœuds de stockage.
- iii. Relancez la procédure de rééquilibrage EC :

```
rebalance-data start --job-id job-id
```

- iv. [Afficher l'état](#) de la nouvelle procédure. Si `State` est toujours `Failure`, contactez le support technique.

7. Si la procédure de rééquilibrage EC génère une charge trop importante (par exemple, les opérations d'ingestion sont affectées), mettez la procédure en pause.

```
rebalance-data pause --job-id job-id
```


8. Si vous devez terminer la procédure de rééquilibrage EC (par exemple, pour une mise à niveau logicielle StorageGRID), entrez ce qui suit :

```
rebalance-data terminate --job-id job-id
```



Lorsque vous terminez une procédure de rééquilibrage EC, tous les fragments de données qui ont déjà été déplacés restent dans leur nouvel emplacement. Les données ne sont pas retransférées à leur emplacement d'origine.

9. Si vous utilisez le code d'effacement sur plusieurs sites, exécutez cette procédure pour tous les autres sites concernés.

Résolution des erreurs d'extension dans StorageGRID

Si vous rencontrez des erreurs pendant le processus d'expansion de grille que vous ne pouvez pas 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. L'accès SSH externe est bloqué par défaut. Si nécessaire, ["autoriser temporairement l'accès"](#) .
2. Se connecter au nœud d'extension qui a rencontré des défaillances :

- a. Saisissez la commande suivante : `ssh -p 8022 admin@grid_node_IP`

Le port 8022 est le port SSH du système d'exploitation de base, tandis que le port 22 est le port SSH du moteur de mise en conteneurs exécutant StorageGRID.

- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Une fois connecté en tant que root, l'invite passe de `$` à `#`.

3. En fonction de la phase d'installation atteinte, récupérez l'un des journaux suivants disponibles sur le nœud de la grille :

Plateforme	Journaux
VMware	• <code>/var/log/daemon.log</code> • <code>/var/log/storagegrid/daemon.log</code> • <code>/var/log/storagegrid/nodes/<node-name>.log</code>

Plateforme	Journaux
Linux	• /var/log/storagegrid/daemon.log • /etc/storagegrid/nodes/<node-name>.conf (pour chaque nœud défaillant) • /var/log/storagegrid/nodes/<node-name>.log (pour chaque nœud défaillant ; peut n'exister)

4. Si vous avez autorisé l'accès SSH externe, "**bloquer l'accès**" lorsque vous avez terminé la tâche.

Maintenance d'un système StorageGRID

Maintenance du grid StorageGRID

Les tâches de maintenance du grid comprennent la désaffectation d'un nœud ou d'un site, le renommage d'une grille, d'un nœud ou d'un site et la maintenance des réseaux. Vous pouvez également effectuer 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® (RHEL), Ubuntu® ou Debian®. Pour une liste des versions prises en charge, consultez le ["Matrice d'interopérabilité NetApp"](#).

Avant de commencer

- Vous avez une bonne compréhension du système StorageGRID.
- Vous avez examiné la topologie de votre système StorageGRID et compris la configuration de la grille.
- Vous comprenez que vous devez suivre toutes les instructions exactement et tenir compte de tous les avertissements.
- Vous comprenez que les procédures de maintenance non décrites ne sont pas prises en charge ou requièrent une mission de service.

Procédures de maintenance des appareils

Pour les procédures matérielles, voir ["Instructions de maintenance pour votre appliance StorageGRID"](#).

Téléchargez le package de récupération StorageGRID

Le fichier de package de récupération vous permet de restaurer le système StorageGRID en cas de panne.

Avant de commencer

- À partir de n'importe quel nœud d'administration, vous êtes connecté au gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez ["autorisations d'accès spécifiques"](#).

Téléchargez le fichier du 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 la mise à niveau du logiciel.

Étapes

1. Sélectionnez **Maintenance > Système > Package de récupération**.
2. Entrez la phrase de passe de provisionnement et sélectionnez **Démarrer le téléchargement**.

Le téléchargement commence immédiatement.

3. Une fois le téléchargement terminé, ouvrez `.zip` le fichier et confirmez que vous pouvez accéder au contenu, y compris au `Passwords.txt` fichier.
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 du système StorageGRID.

Désaffectez les nœuds ou le site

Mettre hors service un nœud ou un site StorageGRID

Vous pouvez effectuer une procédure de mise hors service pour supprimer définitivement les nœuds grid ou un site entier du système StorageGRID.

Pour supprimer un nœud de grille ou un site, effectuez l'une des procédures de mise hors service suivantes :

- Effectuez une pour supprimer un ["désaffectation du nœud grid"](#) ou plusieurs nœuds, qui peuvent se trouver sur un ou plusieurs sites. Les nœuds que vous supprimez peuvent être en ligne et connectés au système StorageGRID, ou encore hors ligne et déconnectés.
- Effectuez une pour supprimer un ["désaffectation du site"](#) site. Vous effectuez une **Désaffected site** si tous les nœuds sont connectés à StorageGRID. Vous effectuez une **Désaffected site** si tous les nœuds sont déconnectés de StorageGRID. Si le site contient une combinaison de nœuds connectés et déconnectés, vous devez remettre tous les nœuds hors ligne en ligne.



Avant de procéder à la désaffectation d'un site déconnecté, contactez votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site. N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer les données d'objet à partir du site.

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. ["Vérifier les travaux de réparation des données"](#).

Désaffectation des nœuds

Mise hors service d'un nœud de la grille StorageGRID

Vous pouvez utiliser la procédure de désaffectation de nœud pour supprimer un ou plusieurs nœuds de grid sur un ou plusieurs sites. Vous ne pouvez pas désaffecter le nœud d'administration principal.

Quand désaffecter un nœud

Utilisez la procédure de mise hors service du nœud lorsque l'un des cas suivants est vrai :

- Vous avez ajouté un nœud de stockage plus grand dans une extension et vous souhaitez supprimer un ou plusieurs nœuds de stockage plus petits tout en préservant les objets.



Si vous souhaitez remplacer une ancienne appliance par une nouvelle, pensez à remplacer une nouvelle appliance par une autre, ["clonage du nœud d'appliance"](#) puis à la mettre hors service.

- Vous avez besoin de moins de stockage total.
- Vous n'avez plus besoin d'un nœud de passerelle.
- Vous n'avez plus besoin d'un nœud d'administration non primaire.
- Votre grille inclut un nœud déconnecté que vous ne pouvez pas restaurer ni remettre en ligne.
- Votre grille inclut un nœud d'archivage.

Comment désaffecter un nœud

Vous pouvez désaffecter les nœuds de grid connectés ou les nœuds de grid déconnectés.

Désaffectation des 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 **Nœuds** et sur la page **Désactiver les nœuds**).

Pour obtenir des instructions, reportez-vous à la section ["Désaffectation des nœuds connectés"](#).

Désaffectation des nœuds déconnectés

Dans certains cas, vous devrez peut-être désaffecter un nœud grid qui n'est pas actuellement connecté à la grille (dont l'état de santé est inconnu ou dont l'état est désactivé sur le plan administratif).

Pour obtenir des instructions, reportez-vous à la section ["Désaffectation des nœuds de la grille déconnectés"](#).

Éléments à prendre en compte avant de désaffecter un nœud

Avant d'effectuer l'une ou l'autre procédure, vérifiez les points à prendre en compte pour chaque type de nœud :

- ["Considérations relatives à la désaffectation d'un nœud d'administration ou de passerelle"](#)
- ["Facteurs à prendre en compte concernant la désaffectation des nœuds de stockage"](#)

Considérations relatives à la mise hors service du nœud Admin ou Gateway StorageGRID

Consultez les considérations relatives à la désaffectation d'un nœud d'administration ou d'un nœud de passerelle.

Considérations relatives au nœud d'administration

- Vous ne pouvez pas désaffecter le nœud d'administration principal.
- Vous ne pouvez pas désaffecter un nœud d'administration si l'une de ses interfaces réseau fait partie d'un groupe haute disponibilité (HA). Vous devez d'abord supprimer les interfaces réseau du groupe haute disponibilité. Voir les instructions pour ["La gestion des groupes de haute disponibilité"](#).
- Si nécessaire, vous pouvez modifier les règles ILM en toute sécurité lors de la désaffectation d'un nœud d'administration.
- Si vous désaffectez un nœud d'administration et que l'authentification unique (SSO) est activée pour votre

système StorageGRID, n'oubliez pas de supprimer la confiance de l'interlocuteur du nœud de Active Directory Federation Services (AD FS).

- Si vous utilisez ["fédération des grilles"](#), assurez-vous que l'adresse IP du nœud que vous désaffecterez n'a pas été spécifiée pour une connexion de fédération de grille.
- Lorsque vous désaffectez un nœud d'administration déconnecté, vous perdrez les journaux d'audit de ce nœud. Cependant, ces journaux doivent également exister sur le nœud d'administration principal.

Considérations relatives au nœud de passerelle

- Vous ne pouvez pas désaffecter un nœud de passerelle si l'une de ses interfaces réseau fait partie d'un groupe haute disponibilité (HA). Vous devez d'abord supprimer les interfaces réseau du groupe haute disponibilité. Voir les instructions pour ["La gestion des groupes de haute disponibilité"](#).
- Vous pouvez modifier les règles ILM en toute sécurité lors de la désaffectation d'un nœud de passerelle.
- Si vous utilisez ["fédération des grilles"](#), assurez-vous que l'adresse IP du nœud que vous désaffecterez n'a pas été spécifiée pour une connexion de fédération de grille.
- Vous pouvez désactiver un nœud de passerelle en toute sécurité lorsqu'il est déconnecté.

Considérations relatives aux nœuds de stockage

Considérations relatives à la mise hors service des nœuds de stockage dans StorageGRID

Avant de désaffecter un nœud de stockage, déterminez si vous pouvez le cloner à la place. Ensuite, si vous décidez de désaffecter le nœud, examinez la façon dont StorageGRID gère les objets et les métadonnées pendant la procédure de désaffectation.

Quand cloner un nœud au lieu de le désaffecter

Si vous souhaitez remplacer un nœud de stockage d'appliance plus ancien par une appliance plus récente ou plus grande, envisagez de cloner le nœud d'appliance au lieu d'ajouter une nouvelle appliance à une extension, puis de désaffecter l'ancienne appliance.

Le clonage des nœuds 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 la nouvelle appliance, met la nouvelle appliance en service et laisse l'ancienne appliance en état de pré-installation.

Il est possible de cloner un nœud d'appliance si vous avez besoin de :

- Remplacez un appareil qui arrive en fin de vie.
- Mettez à niveau un nœud existant pour bénéficier d'une meilleure technologie d'appliance.
- Augmentez la capacité de stockage de grille sans modifier le nombre de nœuds de stockage dans votre système StorageGRID.
- Améliorer l'efficacité du stockage, par exemple en changeant de mode RAID.

Voir ["Clonage de nœuds d'appliance"](#) pour plus de détails.

Considérations relatives aux nœuds de stockage connectés

Consultez les considérations relatives à la désaffectation d'un nœud de stockage connecté.

- Vous ne devez pas désaffecter plus de 10 nœuds de stockage dans une procédure de nœud de mise hors service unique.
- Le système doit, à tout moment, comporter suffisamment de nœuds de stockage pour répondre aux exigences opérationnelles, y compris le ["Quorum ADC"](#) et l'["Politique ILM"](#) actif. Si une mise hors service devait faire passer le nombre d'ADC d'un site en dessous du quorum, StorageGRID déplace automatiquement le service ADC vers des nœuds de stockage non-ADC disponibles sur le même site, maintenant ainsi le quorum ADC. Si le service ADC ne peut pas être déplacé automatiquement, vous devrez peut-être ["ajouter un nouveau nœud de stockage dans une opération d'expansion"](#) avant de pouvoir mettre hors service un nœud de stockage existant.

Soyez prudent lorsque vous désaffectez des nœuds de stockage dans un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section ["Types de nœuds de stockage"](#).

- Lorsque vous supprimez un nœud de stockage, de grands volumes de données d'objet sont transférés sur le réseau. Ces transferts ne doivent pas affecter le fonctionnement normal du système, mais ils peuvent affecter la quantité totale de bande passante réseau consommée par le système StorageGRID.
- Les tâches associées à la mise hors service des nœuds de stockage ont une priorité inférieure aux tâches associées aux opérations normales du système. Cette mise hors service n'interfère pas avec le fonctionnement normal du système StorageGRID et n'a pas besoin d'être planifiée pour une période d'inactivité du système. Comme le déclassement est effectué en arrière-plan, il est difficile d'estimer la durée du processus. En général, la mise hors service s'effectue plus rapidement lorsque le système est silencieux, ou lorsqu'un seul nœud de stockage est retiré à la fois.
- La mise hors service d'un nœud de stockage peut prendre plusieurs jours, voire des semaines. Planifier cette procédure en conséquence. Bien que le processus de mise hors service soit conçu pour ne pas affecter le fonctionnement du système, il peut limiter d'autres procédures. En général, les mises à niveau ou les extensions du système doivent être effectuées avant de supprimer les nœuds grid.
- Si vous devez effectuer une autre procédure de maintenance pendant la suppression des nœuds de stockage, vous pouvez ["interrompre la procédure de mise hors service"](#) la reprendre une fois l'autre procédure terminée.



Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan.

- Vous ne pouvez pas exécuter les opérations de réparation des données sur des nœuds de grille lorsqu'une tâche de désaffectation est en cours d'exécution.
- Vous ne devez apporter aucune modification à une règle ILM pendant la désaffectation d'un nœud de stockage.
- Pour supprimer définitivement et de manière sécurisée des données, vous devez effacer les disques du nœud de stockage une fois la procédure de mise hors service terminée.

Considérations relatives aux nœuds de stockage déconnectés

Consultez les considérations relatives à la désaffectation d'un nœud de stockage déconnecté.

- Ne désaffectez jamais un nœud déconnecté, sauf si vous êtes sûr qu'il ne peut pas être mis en ligne ou restauré.



N'effectuez pas cette procédure si vous pensez qu'il est possible de récupérer des données d'objet à partir du nœud. Contactez plutôt le support technique pour déterminer si la restauration du nœud est possible.

- Lorsque vous désaffectez un nœud de stockage déconnecté, StorageGRID utilise les données d'autres nœuds de stockage pour reconstruire les données d'objet et les métadonnées qui se trouvent sur le nœud déconnecté.
- Une perte de données peut se produire si vous mettez hors service plusieurs nœuds de stockage déconnectés. Il se peut que le système ne puisse pas reconstruire les données si les copies d'objet, les fragments avec code d'effacement ou les métadonnées d'objet restent disponibles. Lors de la désaffectation des nœuds de stockage dans une grille avec des nœuds de métadonnées uniquement basés sur le logiciel, la désaffectation de tous les nœuds configurés pour stocker à la fois des objets et des métadonnées supprime tout le stockage objet de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section "[Types de nœuds de stockage](#)".



Si vous ne pouvez pas restaurer plusieurs nœuds de stockage déconnectés, contactez le support technique pour déterminer la meilleure solution.

- Lorsque vous désaffectez un nœud de stockage déconnecté, StorageGRID démarre les tâches de réparation des données à la fin du processus de désaffectation. Ces travaux tentent de reconstruire les données d'objet et les métadonnées stockées sur le nœud déconnecté.
- Lorsque vous désaffectez un nœud de stockage déconnecté, la procédure de mise hors service se termine relativement rapidement. Cependant, les tâches de réparation des données peuvent prendre des jours ou des semaines et ne sont pas surveillées par la procédure de mise hors service. Vous devez contrôler ces travaux manuellement et les redémarrer au besoin. Voir "[Vérifier les travaux de réparation des données](#)".
- Si vous désaffectez un nœud de stockage déconnecté qui contient la seule copie d'un objet, celui-ci sera perdu. Les tâches de réparation des données ne peuvent reconstruire et récupérer que des objets si au moins une copie répliquée ou suffisamment de fragments avec code d'effacement existent sur les nœuds de stockage actuellement connectés.

Qu'est-ce que le quorum ADC de StorageGRID ?

Le quorum ADC garantit qu'un nombre minimal de services de contrôleur de domaine administratif (ADC) reste disponible sur chaque site. StorageGRID déplace automatiquement le service ADC lors de la mise hors service, si nécessaire.

Le service ADC, qui se trouve 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 que le quorum des services ADC soit disponible sur chaque site et à tout moment.

Vous ne pouvez pas désaffecter un nœud de stockage si le retrait du nœud entraînerait la non-conformité du quorum ADC. Pour satisfaire au quorum ADC lors d'une mise hors service, au moins 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 un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section "[Types de nœuds de stockage](#)".

Supposons par exemple qu'un site comprend actuellement six nœuds de stockage avec des services ADC et que vous souhaitez désaffecter trois nœuds de stockage. En raison de l'exigence de quorum ADC, vous devez effectuer deux procédures de mise hors service, comme suit :

- Dans la première procédure de mise hors service, vous devez vous assurer que quatre nœuds de stockage avec services ADC restent disponibles : $((0.5 * 6) + 1)$. Cela signifie que vous ne pouvez désaffecter que deux nœuds de stockage au départ.
- 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 : $((0.5 * 4) + 1)$.

Lors de la mise hors service d'un nœud de stockage hébergeant le service ADC, StorageGRID transfère automatiquement ce service vers un autre nœud de stockage du même site si cette mise hors service ramène le nombre de nœuds ADC du site en dessous du quorum. Ce transfert automatique nécessite que tous les nœuds du grid soient connectés et que des nœuds de stockage non-ADC soient disponibles sur le même site pour recevoir le service. La procédure de mise hors service garantit un minimum de trois nœuds de stockage ADC par site. Par exemple, si vous mettez hors service quatre ou six nœuds ADC sur un site, trois nœuds de stockage ADC resteront après la procédure, à condition que des nœuds non-ADC soient disponibles sur le même site.

Si le service ADC ne peut pas être déplacé automatiquement, vous pouvez ["déplacer manuellement le service ADC"](#) le déplacer vers un autre nœud de stockage du même site ou ["ajouter un nouveau nœud de stockage dans une extension"](#) spécifier qu'il doit héberger un service ADC. Vous pouvez ensuite mettre hors service le nœud de stockage existant sans affecter le quorum.

Examinez la politique ILM de StorageGRID et la configuration de stockage

Si vous prévoyez de désaffecter un nœud de stockage, nous vous recommandons de consulter la politique ILM de votre système StorageGRID avant de lancer le processus de désaffectation.

Pendant la mise hors service, toutes les données d'objet sont migrées du nœud de stockage hors service vers d'autres nœuds de stockage.



La politique ILM que vous avez *pendant* la mise hors service sera celle utilisée *après* la mise hors service. Vous devez vous assurer que cette règle répond à vos besoins en matière de données avant la mise hors service et une fois la mise hors service terminée.

Vous devez passer en revue les règles de chacun ["Règle ILM active"](#) pour vous assurer que le système StorageGRID continuera à avoir une capacité suffisante du type correct et aux emplacements appropriés pour permettre la mise hors service d'un nœud de stockage.

Tenez compte des points suivants :

- Sera-t-il possible que les services d'évaluation ILM copient les données d'objet si les règles ILM sont respectées ?
- Que se passe-t-il si un site devient temporairement indisponible pendant la mise hors service ? Des copies supplémentaires peuvent-elles être effectuées dans un autre emplacement ?
- En quoi le processus de mise hors service aura-t-il une incidence sur la distribution finale du contenu ? Comme décrit à la section ["Consolidez les nœuds de stockage"](#), vous devez ["Ajout de nœuds de stockage"](#) avant de mettre hors service les anciens. Si vous ajoutez un nœud de stockage de remplacement plus grand après avoir désaffectant un nœud de stockage plus petit, les anciens nœuds de

stockage peuvent être proches de leur capacité et le nouveau nœud de stockage n'aurait presque pas de contenu. La plupart des opérations d'écriture des nouvelles données d'objet sont ensuite dirigées vers le nouveau nœud de stockage, ce qui réduit l'efficacité globale des opérations système.

- Le système inclura-t-il à tout moment suffisamment de nœuds de stockage pour satisfaire aux règles ILM actives ?



Une règle ILM insatisfaite peut entraîner des backlogs et des alertes et peut arrêter le fonctionnement du système StorageGRID.

Vérifiez que la topologie proposée qui résultera du processus de désaffectation respecte la politique ILM en évaluant les zones répertoriées dans le tableau.

Domaine à évaluer	Que faut-il prendre en compte
Capacité disponible	Y aura-t-il une capacité de stockage suffisante pour prendre en charge 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'objet stockées pendant un délai raisonnable après la fin de la mise hors service ?
Emplacement de stockage	Si la capacité reste dans l'ensemble du système StorageGRID, la capacité est-elle suffisante aux bons emplacements afin de satisfaire aux règles métier du système StorageGRID ?
Type de stockage	Y aura-t-il suffisamment de stockage pour le type approprié une fois la mise hors service terminée ? Par exemple, les règles ILM peuvent déplacer le 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 StorageGRID

Vous pouvez consolider les nœuds de stockage pour réduire le nombre de nœuds de stockage sur un site ou un déploiement, tout en augmentant la capacité de stockage.

Lorsque vous consolidez les nœuds de stockage, vous ajoutez de nouveaux nœuds de stockage de plus grande capacité, puis vous ["Développez le système StorageGRID"](#) désaffectez les anciens nœuds de stockage de plus petite capacité. Pendant la procédure de mise hors service, les objets sont migrés entre les anciens nœuds de stockage et les nouveaux nœuds de stockage.



Si vous consolidez des appliances plus anciennes ou plus petites avec de nouveaux modèles ou des appliances de plus grande capacité, envisagez d'utiliser (ou le clonage des nœuds de l'appliance et la procédure de désaffectation si vous ne remplacez pas les appliances ["clonage du nœud d'appliance"](#) un-à-un).

Par exemple, vous pouvez ajouter deux nouveaux nœuds de stockage de plus grande capacité pour remplacer trois nœuds de stockage plus anciens. Vous devez d'abord utiliser la procédure d'extension pour ajouter les deux nouveaux nœuds de stockage de plus grande capacité, puis éliminer les trois anciens nœuds de stockage de plus grande capacité.

Lorsque vous ajoutez de la capacité supplémentaire avant de supprimer les nœuds de stockage, vous assurez une distribution plus équilibrée des données sur le système StorageGRID. Vous réduisez également la possibilité qu'un nœud de stockage existant soit repoussé au-delà du niveau du filigrane.

Mise hors service de plusieurs nœuds de stockage StorageGRID

Si vous devez supprimer plusieurs nœuds de stockage, vous pouvez les désaffecter de manière séquentielle ou parallèle.



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section "[Types de nœuds de stockage](#)".

- Si vous mettez hors service les nœuds de stockage de façon séquentielle, vous devez attendre la fin du déclassé du premier nœud de stockage avant de procéder à la mise hors service du prochain nœud de stockage.
- Si vous mettez hors service les nœuds de stockage en parallèle, les nœuds de stockage traitent simultanément les tâches de désaffectation de tous les nœuds de stockage qui sont désaffectés. Cela peut entraîner 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.

Consultez les tâches de réparation de données dans StorageGRID

Avant de mettre hors service ou d'étendre 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.

- Se référer à "[Types d'extension](#)" pour plus de détails sur la façon d'étendre un nœud de grille.
- Utilisez le Gestionnaire de grille pour suivre les processus de restauration en cours et afficher l'historique des restaurations. Consultez ces procédures :
 - "[Restaurez les données d'objet vers un volume de stockage pour l'appliance](#)"
 - "[Restaurez les données d'objet vers le volume de stockage sur lequel le disque système est intact](#)"
 - "[Restauration des données d'objet sur le volume de stockage \(panne de disque système\)](#)"

Rassemblez les matériaux nécessaires pour la mise hors service du nœud StorageGRID

Avant d'effectuer la mise hors service d'un nœud de la grille, vous devez obtenir les informations suivantes.

Élément	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 de package de récupération pour restaurer le système en cas de panne.
Passwords.txt fichier	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.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement ne se trouve pas dans Passwords.txt le fichier.
Description de la topologie du système StorageGRID avant la mise hors service	Le cas échéant, procurez-vous toute documentation décrivant la topologie actuelle du système.

Informations associées

["Navigateurs Web pris en charge"](#)

Accédez à la page Décommissionnement des nœuds dans StorageGRID

Lorsque vous accédez à la page Decommission Nodes dans Grid Manager, vous pouvez voir en un coup d'œil quels nœuds peuvent être désaffectés.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section ["Types de nœuds de stockage"](#).

Étapes

1. Sélectionnez **Maintenance > Tâches > Mise hors service**.
2. Sélectionnez **nœuds de mise hors service**.

La page nœuds de mise hors service s'affiche. À partir de cette page, vous pouvez :

- Déterminez les nœuds de la grille qui peuvent être désaffectés.
- Voir l'état de santé de tous les nœuds de la grille
- Triez la liste par ordre croissant ou décroissant en fonction de **Nom**, **site**, **Type** ou **a ADC**.
- Entrez des termes de recherche pour trouver rapidement des nœuds spécifiques.

Dans cet exemple, une coche verte dans la colonne « Désactivation possible » indique que vous pouvez désactiver le nœud API Gateway et le nœud de stockage de données uniquement. Les autres nœuds ne peuvent pas être désactivés pour diverses raisons. Par exemple, le nœud d'administration principal ne peut pas être désactivé car la désactivation de ce type de nœud n'est pas prise en charge. Le nœud de stockage de métadonnées uniquement ne peut pas être désactivé car le site ne répondrait plus aux "Quorum ADC".

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-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node (Metadata-only)	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
☐ DC1-S4	Data Center 1	Storage Node (Data-only)	No		
DC2-ADM1	Data Center 2	Admin Node	-		No, member of HA group(s); HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.

3. Consultez la colonne **Decommission possible** pour chaque nœud que vous souhaitez désaffecter.

Si un nœud de grid peut être désaffecté, cette colonne est cochée en vert, et la colonne de gauche inclut une case à cocher. Si un nœud ne peut pas être désaffecté, cette colonne décrit le problème. S'il existe plusieurs raisons pour lesquelles un nœud ne peut pas être désaffecté, la raison la plus critique s'affiche.

Motif de mise hors service possible	Description	Étapes à résoudre
Non, <i>node type</i> désaffectation n'est pas pris en charge.	Vous ne pouvez pas désaffecter le nœud d'administration principal.	Aucune.
Non, au moins un nœud de la grille est déconnecté. Remarque : ce message s'affiche uniquement pour les nœuds de réseau connectés.	Vous ne pouvez pas désaffecter un nœud de grid connecté si un nœud de grid est déconnecté. La colonne Santé comprend l'une des icônes suivantes pour les nœuds de grille déconnectés :  (gris) : Administrativement désactivé  (bleu) : Inconnu	Vous devez remettre tous les nœuds déconnectés en ligne ou "déclassez tous les nœuds déconnectés" avant de pouvoir supprimer un nœud connecté. Remarque : si votre grille contient plusieurs nœuds déconnectés, le logiciel vous demande de les désaffecter tous en même temps, ce qui augmente le potentiel de résultats inattendus.

Motif de mise hors service possible	Description	Étapes à résoudre
Non, un ou plusieurs nœuds requis sont actuellement déconnectés et doivent être restaurés. Remarque : ce message s'affiche uniquement pour les nœuds de grille déconnectés.	Vous ne pouvez pas désaffecter un nœud de grille déconnecté si un ou plusieurs nœuds requis sont également déconnectés (par exemple, un nœud de stockage requis pour le quorum ADC).	- Consultez les messages de mise hors service possibles pour tous les nœuds déconnectés. - Déterminez les nœuds qui ne peuvent pas être désaffectés, car ils sont requis. - Si l'état de santé d'un nœud requis est désactivé d'un point de vue administratif, remettre le nœud en ligne. - Si l'état de santé d'un nœud requis n'est pas connu, effectuez une procédure de restauration de nœud pour restaurer le nœud requis.
Non, membre du groupe 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 désaffecter un nœud d'administration ou un nœud de passerelle si une interface de nœud appartient à un groupe haute disponibilité (HA).	Modifiez le groupe haute disponibilité pour supprimer l'interface du nœud ou supprimer l'ensemble du groupe haute disponibilité. Voir "Configurez les groupes haute disponibilité".
Non, le site x nécessite au moins 3 nœuds de stockage avec services ADC ou des nœuds non-ADC disponibles pour y transférer les services ADC. La mise hors service d'un nœud ADC n'est pas disponible si des nœuds sont hors ligne.	Nœuds de stockage uniquement (nœuds de stockage combinés ou de métadonnées uniquement). Vous ne pouvez pas mettre hors service un nœud de stockage si le nombre de nœuds restants sur le site est insuffisant pour respecter les exigences de quorum de l'ADC et si le service ADC ne peut pas être déplacé automatiquement. Le déplacement automatique nécessite la présence de plus de deux nœuds de stockage ADC en ligne sur la grille et de nœuds de stockage non-ADC disponibles sur le même site.	Assurez-vous que les conditions pour le déplacement automatique du service ADC sont remplies (voir "Quorum ADC"), ou "déplacer manuellement le service ADC" vers un autre nœud de stockage sur le même site. Vous pouvez également effectuer une extension en ajoutant un nouveau nœud de stockage au site et en spécifiant qu'il doit avoir un service ADC. Voir "Résumé du workflow d'ajout de nœuds de grille à StorageGRID".

Motif de mise hors service possible	Description	Étapes à résoudre
Non, un ou plusieurs profils de code d'effacement nécessitent au moins n nœuds de stockage. Si le profil n'est pas utilisé dans une règle ILM, vous pouvez le désactiver.	Nœuds de stockage uniquement. Vous ne pouvez pas 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 code d'effacement existe pour un code d'effacement 4+2, au moins 6 nœuds de stockage doivent rester.	Pour chaque profil de code d'effacement concerné, effectuez l'une des opérations suivantes en fonction de l'utilisation du profil : • Utilisé dans les stratégies ILM actives : effectuer une extension. Ajoutez suffisamment de nœuds de stockage pour que le code d'effacement puisse continuer. Voir les instructions pour "extension de votre grille". • Utilisé dans une règle ILM, mais pas dans des règles ILM actives : modifiez ou supprimez la règle, puis désactivez le profil de code d'effacement. • Non utilisé dans une règle ILM : désactive le profil de code d'effacement. Remarque : un message d'erreur s'affiche si vous tentez de désactiver un profil de code d'effacement et que les données d'objet sont toujours associées au profil. Vous devrez peut-être attendre plusieurs semaines avant d'essayer à nouveau le processus de désactivation. En savoir plus sur "désactivation d'un profil de code d'effacement".
Non, vous ne pouvez pas désaffecter un nœud d'archivage à moins que le nœud ne soit déconnecté.	Si un nœud d'archivage est toujours connecté, vous ne pouvez pas le supprimer.	Remarque : la prise en charge des nœuds d'archivage a été supprimée. Si vous devez désaffecter un nœud d'archivage, reportez-vous à la section "Désaffectation du nœud grid (site du doc StorageGRID 11.8)"

Mettre hors service les nœuds StorageGRID déconnectés

Vous devrez peut-être désaffecter un nœud qui n'est pas actuellement connecté à la grille (dont l'état de santé est inconnu ou désactivé d'un point de vue administratif).

Avant de commencer

- Vous comprenez les 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'aucun travail de réparation de données n'est actif. Voir "[Vérifier les travaux de réparation des données](#)".
- Vous avez confirmé que la restauration du nœud de stockage n'est pas en cours dans la grille. Si c'est le cas, vous devez attendre que la reconstruction Cassandra soit terminée. Vous pouvez ensuite procéder au déclassement.
- Vous avez vérifié que d'autres procédures de maintenance ne seront pas exécutées alors que la procédure de mise hors service du nœud est en cours d'exécution, à moins que la procédure de mise hors service du nœud soit interrompue.
- La colonne **Decommission possible** pour le ou les nœuds déconnectés que vous souhaitez désaffecter contient une coche verte.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Vous pouvez identifier les nœuds déconnectés en recherchant l'icône bleue Inconnu  ou l'icône grise Administrativement hors service  dans la colonne **Santé**.

Avant de désaffecter un nœud déconnecté, notez ce qui suit :

- Cette procédure est principalement destinée à supprimer un seul nœud déconnecté. Si votre grille contient plusieurs nœuds déconnectés, le logiciel requiert que vous les désins affectez 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 un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section "[Types de nœuds de stockage](#)".

- 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. Sauf si vous désaffectez un nœud d'archivage (qui doit être déconnecté), essayez de remettre en ligne ou de restaurer les nœuds de grille déconnectés.

Voir "[Procédures de restauration des nœuds de la grille](#)" pour obtenir des instructions.

2. Si vous ne pouvez pas restaurer un nœud de grid déconnecté et que vous souhaitez le désaffecter alors qu'il est déconnecté, cochez la case correspondant à ce nœud.



Si votre grille contient plusieurs nœuds déconnectés, le logiciel requiert que vous les désinsaffectez tous en même temps, ce qui augmente le risque de résultats inattendus.



Soyez prudent lorsque vous choisissez de désaffecter plusieurs nœuds de grid déconnectés à la fois, en particulier si vous sélectionnez plusieurs nœuds de stockage déconnectés. Si vous ne pouvez pas restaurer plusieurs nœuds de stockage déconnectés, contactez le support technique pour déterminer la meilleure solution.

3. Saisissez la phrase secrète pour le provisionnement.

Le bouton **Start Decommission** est activé.

4. Sélectionnez **Démarrer la mise hors service**.

Un avertissement apparaît, indiquant que vous avez sélectionné un nœud déconnecté et que ces données d'objet seront perdues si le nœud possède la seule copie d'un objet.

5. Examinez la liste des nœuds, puis sélectionnez **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, sélectionnez le lien ou sélectionnez **Maintenance > System > Recovery package** pour accéder à la page du package de récupération. Téléchargez ensuite le .zip fichier.

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 du système StorageGRID.

7. Surveillez régulièrement la page mise hors service pour vous assurer que tous les nœuds sélectionnés sont correctement mis hors service.

La désaffectation des nœuds de stockage peut prendre plusieurs jours ou semaines. Lorsque toutes les tâches sont terminées, la liste de sélection de nœud apparaît à nouveau avec un message de réussite. Si vous avez désactivé un nœud de stockage déconnecté, un message d'information indique que les tâches de réparation ont été lancées.

8. Une fois les nœuds arrêtés automatiquement dans le cadre de la procédure de mise hors service, supprimez les machines virtuelles restantes ou d'autres ressources associées au nœud mis hors service.



N'effectuez pas cette étape tant que les nœuds ne s'arrêtent pas automatiquement.

9. Si vous mettez hors service un nœud de stockage, surveillez l'état des tâches de réparation des **données répliquées** et des **données à codage d'effacement (EC)** qui sont automatiquement lancées pendant le processus de mise hors service.

Les données répliquées

- Pour déterminer si les réparations sont terminées :
 - i. Sélectionnez **Nœuds** > **Nœud de stockage en cours de réparation** > **ILM**.
 - ii. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
 - i. Sélectionnez **Nœuds**.
 - ii. Sélectionnez **grid name** > **ILM**.
 - iii. Placez votre curseur sur le graphique de la file d'attente ILM pour voir la valeur de l'attribut **Taux d'analyse (objets/sec)**, qui est le taux auquel les objets de la grille sont analysés et mis en file d'attente pour ILM.
 - iv. Dans la section File d'attente ILM, examinez les attributs suivants :
 - **Période d'analyse - estimation** : 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 tentées pour les données répliquées considérées comme à haut risque. Les objets à haut risque sont tous les objets avec une copie restante, qu'elle soit spécifiée par la politique ILM ou à la suite de copies perdues. 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.
 - v. Vous pouvez également soumettre une requête Prometheus pour `storagegrid_ilm_scan_period_estimated_minutes` et `storagegrid_ilm_repairs_attempted`.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données à code d'effacement et relancer toute requête qui aurait pu échouer, 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 **Grid EC Job Estimated Time to Completion** et **Grid EC Job Percentage Completed**.

Une fois que vous avez terminé

Dès que les nœuds déconnectés ont été désaffectés et que toutes les tâches de réparation de données ont été effectuées, vous pouvez désaffecter tous les nœuds de la grille connectés si nécessaire.

Ensuite, procédez comme suit après avoir effectué la procédure de mise hors service :

- Assurez-vous que les disques du nœud de la grille mis hors service sont nettoyés. Utilisez un outil ou un

service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.

- Si vous désaffecté un nœud d'appliance et que les données de l'appliance étaient protégées à l'aide du chiffrement des nœuds, utilisez le programme d'installation de l'appliance StorageGRID pour effacer la configuration du serveur de gestion des clés (KMS transparent). Vous devez effacer la configuration KMS si vous souhaitez ajouter l'appliance à une autre grille. Pour obtenir des instructions, reportez-vous à la section ["Surveillez le chiffrement des nœuds en mode de maintenance"](#).

Mettre hors service les nœuds StorageGRID connectés

Vous pouvez mettre hors service et supprimer définitivement les nœuds connectés à la grille.

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 réuni tous les documents requis.
- Vous avez vérifié qu'aucun travail de réparation de données n'est actif.
- Vous avez confirmé que la restauration du nœud de stockage n'est pas en cours dans la grille. Si c'est le cas, attendez que toute reconstruction Cassandra effectuée dans le cadre de la restauration soit terminée. Vous pouvez ensuite procéder au déclassement.
- Vous avez vérifié que d'autres procédures de maintenance ne seront pas exécutées alors que la procédure de mise hors service du nœud est en cours d'exécution, à moins que la procédure de mise hors service du nœud soit interrompue.
- Vous avez la phrase secrète pour le provisionnement.
- Les nœuds de la grille sont connectés.
- La colonne **décomposition possible** du ou des nœuds que vous souhaitez désaffecter comporte une coche verte.



La mise hors service ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.



Si un ou plusieurs volumes sont déconnectés alors qu'une mise hors service est en cours, le processus de mise hors service se termine une fois ces volumes remis en ligne.

- Tous les nœuds de la grille ont un état normal (vert) . Si vous voyez l'une de ces icônes dans la colonne **État**, vous devez essayer de résoudre le problème :

Icône	Couleur	Gravité
	Jaune	Avertissement
	Orange clair	Mineur
	Orange foncé	Majeur

Icône	Couleur	Gravité
	Rouge	Primordial

- Si vous avez précédemment mis hors service un nœud de stockage déconnecté, les tâches de réparation des données ont toutes été effectuées avec succès. Voir "[Vérifier les travaux de réparation des données](#)".



Ne supprimez pas la machine virtuelle ou d'autres ressources d'un nœud de grille avant d'y être invité dans cette procédure.



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans un grid contenant des nœuds de métadonnées uniquement basés sur des logiciels. Si vous désaffectez tous les nœuds configurés pour stocker *les deux* objets et les métadonnées, la capacité de stockage des objets est supprimée de la grille. Pour plus d'informations sur les nœuds de stockage des métadonnées uniquement, reportez-vous à la section "[Types de nœuds de stockage](#)".

Description de la tâche

Lorsqu'un nœud est désaffecté, ses services sont désactivés et le nœud s'arrête automatiquement.

Étapes

1. Dans la page nœuds de décomposition, cochez la case correspondant à chaque nœud de grille que vous souhaitez désaffecter.
2. Saisissez la phrase secrète pour le provisionnement.

Le bouton **Start Decommission** est activé.

3. Sélectionnez **Démarrer la désaffectation**.
4. Vérifiez 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 après le démarrage de la procédure de mise hors service. La modification de l'état peut entraîner l'absence de copie de contenu vers d'autres emplacements.

5. Dès que le nouveau package de récupération est disponible, sélectionnez le lien du package de récupération dans la bannière ou sélectionnez **Maintenance > Système > Package de récupération** pour accéder à la page du package de récupération. 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 nœuds de mise hors service pour vous assurer que tous les nœuds sélectionnés sont correctement mis hors service.



La désaffectation des nœuds de stockage peut prendre plusieurs jours ou semaines.

Lorsque toutes les tâches sont terminées, la liste de sélection de nœud apparaît à nouveau avec un message de réussite.

Une fois que vous avez terminé

Suivez cette procédure une fois la procédure de mise hors service du nœud terminée :

1. Suivez l'étape appropriée pour votre plate-forme. 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 des nœuds logiciels"](#).
 - **VMware** : vous pouvez utiliser l'option " Supprimer du disque " de vCenter pour supprimer la machine virtuelle. Il se peut également que vous deviez supprimer tous les disques de données qui sont indépendants de la machine virtuelle.
 - **Appliance StorageGRID** : le nœud de l'appliance revient automatiquement à un état non déployé où vous pouvez accéder au programme d'installation de l'appliance StorageGRID. Vous pouvez mettre l'appareil hors tension ou l'ajouter à un autre système StorageGRID.
2. Assurez-vous que les disques du nœud de la grille mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.
3. Si vous désaffecté un nœud d'appliance et que les données de l'appliance étaient protégées à l'aide du chiffrement des nœuds, utilisez le programme d'installation de l'appliance StorageGRID pour effacer la configuration du serveur de gestion des clés (KMS transparent). Vous devez effacer la configuration KMS si vous souhaitez ajouter l'appliance à une autre grille. Pour obtenir des instructions, reportez-vous à la section ["Surveillez le chiffrement des nœuds en mode de maintenance"](#).

Mettre en pause et reprendre le processus de mise hors service des nœuds de stockage StorageGRID

Si vous devez effectuer une deuxième procédure de maintenance, vous pouvez interrompre la procédure de mise hors service d'un nœud de stockage pendant certaines étapes. Une fois l'autre procédure terminée, vous pouvez reprendre la mise hors service.



Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).

Étapes

1. Sélectionnez **Maintenance > Tâches > Mise hors service**.

La page mise hors service s'affiche.

2. Sélectionnez **nœuds de mise hors service**.

La page nœuds de mise hors service s'affiche. Lorsque la procédure de mise hors service atteint l'une des étapes suivantes, le bouton **Pause** est activé.

- Évaluation des règles ILM

- Déclassement des données avec code d'effacement

3. Sélectionnez **Pause** pour suspendre la procédure.

L'étape en cours est mise en pause et le bouton **reprendre** est activé.

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 Q				
Name	Type	Progress	Stage	
DC1-S5	Storage Node		Evaluating ILM	

Pause

Resume

4. Une fois l'autre procédure de maintenance terminée, sélectionnez **reprendre** pour poursuivre la mise hors service.

Désaffecter le site

Considérations relatives à la mise hors service des sites dans StorageGRID

Avant d'utiliser la procédure de mise hors service du site pour supprimer un site, vous devez prendre en compte les considérations.

Que se passe-t-il lorsque vous désaffectez un site

Lorsque vous désaffectez un site, StorageGRID supprime définitivement tous les nœuds du site et le site lui-même du système StorageGRID.

Lorsque la procédure de mise hors service du site est terminée :

- Vous ne pouvez plus utiliser StorageGRID pour afficher ou accéder au site ou à l'un des nœuds du site.
- Vous ne pouvez plus utiliser de pools de stockage ou de profils de code d'effacement faisant référence au site. Lorsque StorageGRID décompresse un site, il supprime automatiquement ces pools de stockage et désactive ces profils de code d'effacement.

Différences entre les procédures de mise hors service du site connecté et du site déconnecté

Vous pouvez utiliser la procédure de mise hors service du site pour supprimer un site dans lequel tous les nœuds sont connectés à StorageGRID (appelé mise hors service du site connecté) ou pour supprimer un site dans lequel tous les nœuds sont déconnectés de StorageGRID (appelé mise hors service hors site déconnectée). Avant de commencer, vous devez comprendre les différences entre ces procédures.



Si un site contient un mélange de nœuds connectés () et de nœuds déconnectés ( ou ) , vous devez remettre en ligne tous les nœuds hors ligne.

- Une désaffectation de site connecté vous permet de supprimer un site opérationnel du système StorageGRID. Par exemple, vous pouvez effectuer une mise hors service du site connecté pour supprimer un site qui fonctionne mais qui n'est plus nécessaire.
- Lorsque StorageGRID supprime un site connecté, il gère les données d'objet du site à l'aide de ILM. Avant de pouvoir lancer la désaffectation d'un site connecté, vous devez supprimer ce site de toutes les règles ILM et activer une nouvelle règle ILM. Les processus ILM pour migrer les données d'objet et les processus internes pour supprimer un site peuvent se produire au même moment, mais la meilleure pratique consiste à exécuter la procédure ILM avant de démarrer la procédure de déclassement.
- Une désaffectation du site vous permet de supprimer un site défectueux du système StorageGRID. Par exemple, vous pouvez effectuer une mise hors service du site déconnecté pour retirer un site qui a été détruit par un incendie ou une inondation.

Lorsque StorageGRID supprime un site déconnecté, il considère que tous les nœuds sont irrécupérables et ne tentent pas de préserver les données. Toutefois, avant de pouvoir démarrer une mise hors service de site déconnecté, vous devez supprimer le site de toutes les règles ILM et activer une nouvelle règle ILM.



Avant d'effectuer une procédure de mise hors service hors site déconnectée, vous devez contacter votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site. N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer les données d'objet à partir du site.

Conditions générales requises pour supprimer un site connecté ou déconnecté

Avant de supprimer un site connecté ou déconnecté, vous devez connaître les exigences suivantes :

- Vous ne pouvez pas désaffecter un site qui inclut le nœud d'administration principal.
- Vous ne pouvez pas désaffecter un site si l'un des nœuds dispose d'une interface appartenant à un groupe haute disponibilité (HA). Vous devez modifier le groupe haute disponibilité pour supprimer l'interface du nœud ou supprimer l'ensemble du groupe haute disponibilité.
- Vous ne pouvez pas mettre hors service un site s'il contient un mélange de nœuds connectés () et déconnectés ( ou ).
- 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 mise hors service du site si une opération de réparation de nœud est en cours. Voir "[Vérifier les travaux de réparation des données](#)" pour suivre les réparations des données avec code d'effacement.
- Pendant que la procédure de mise hors service du site est en cours d'exécution :
 - Vous ne pouvez pas créer de règles ILM faisant référence au site en cours de désaffectation. Vous ne pouvez pas non plus modifier une règle ILM existante pour faire référence au site.
 - Vous ne pouvez pas effectuer d'autres procédures de maintenance, telles que l'extension ou la mise à niveau.



Si vous devez effectuer une autre procédure de maintenance pendant une mise hors service d'un site connecté, vous pouvez ["Interrompez la procédure pendant le retrait des nœuds de stockage"](#). Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan. Une fois la deuxième procédure d'entretien terminée, vous pouvez reprendre la mise hors service.

- Si vous devez récupérer un nœud après avoir lancé la procédure de mise hors service du site, vous devez contacter le service de support.
- Vous ne pouvez pas désaffecter plusieurs sites à la fois.
- Si le site inclut un ou plusieurs nœuds d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, vous devez supprimer toutes les approbations tierces pour le site de Active Directory Federation Services (AD FS).

Exigences relatives à la gestion du cycle de vie des informations (ILM)

Dans le cadre de la suppression d'un site, vous devez mettre à jour votre configuration ILM. L'assistant dédié au site de désaffectation vous guide à travers un certain nombre d'étapes préalables pour vous assurer que :

- Le site n'est référencé par aucune politique ILM. Le cas échéant, vous devez modifier les règles ou créer et activer des règles avec de nouvelles règles ILM.
- Aucune règle ILM ne renvoie au site, même si ces règles ne sont utilisées dans aucune règle. Vous devez supprimer ou modifier toutes les règles qui font référence au site.

Lorsque StorageGRID décompresse le site, il désactive automatiquement les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Si le pool de stockage tous les nœuds existe (StorageGRID 11.6 et versions antérieures), il est supprimé car il utilise tous les sites.



Avant de pouvoir supprimer un site, vous devrez peut-être créer de nouvelles règles ILM et activer une nouvelle politique ILM. Ces instructions supposent que vous connaissez bien le fonctionnement d'ILM et que vous connaissez déjà la création de pools de stockage, les profils de code d'effacement, les règles ILM, ainsi que la simulation et l'activation d'une stratégie ILM. Voir ["Gestion des objets avec ILM"](#).

Considérations relatives aux données d'objet sur un site connecté

Si vous effectuez la mise hors service d'un site connecté, vous devez décider ce que vous devez faire avec les données d'objet existantes sur le site lorsque vous créez de nouvelles règles ILM et une nouvelle règle ILM. Vous pouvez effectuer l'une des opérations suivantes ou les deux :

- Déplacez les données d'objet du site sélectionné vers un ou plusieurs autres sites de votre grille.

Exemple de déplacement de données : supposons que vous souhaitiez désaffecter un site à Raleigh parce que vous avez ajouté un nouveau site à Sunnyvale. Dans cet exemple, vous voulez déplacer toutes les données d'objet de l'ancien site vers le nouveau site. Avant de mettre à jour vos règles ILM et vos règles ILM, vous devez vérifier la capacité sur les deux sites. Vous devez vous assurer que la capacité du site de Sunnyvale est suffisante pour prendre en charge les données objet depuis le site Raleigh, et que la capacité nécessaire à sa croissance future restera celle de Sunnyvale.



Pour assurer la disponibilité d'une capacité adéquate, il peut être nécessaire d'"développez une grille"ajouter des volumes de stockage ou des nœuds de stockage à un site existant ou d'ajouter un nouveau site avant d'effectuer cette procédure.

- Supprimer les copies d'objet du site sélectionné.

Exemple de suppression de données : supposons que vous utilisez actuellement une règle ILM de 3 copies pour répliquer des données d'objet sur trois sites. Avant de désaffecter un site, vous pouvez créer une règle ILM à 2 copies pour stocker les données sur seulement deux sites. Lorsque vous activez une nouvelle règle ILM utilisant la règle à 2 copies, StorageGRID supprime les copies du troisième site car elles ne satisfont plus aux exigences ILM. Cependant, les données d'objet seront toujours protégées et la capacité des deux sites restants restera identique.



Ne créez jamais de règle ILM à copie unique pour la suppression d'un site. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Exigences supplémentaires relatives à la mise hors service d'un site connecté

Avant que StorageGRID puisse supprimer un site connecté, vous devez vous assurer que :

- Tous les nœuds de votre système StorageGRID doivent avoir un état de connexion **Connecté** (✓); cependant, les nœuds peuvent avoir des alertes actives.



Vous pouvez exécuter les étapes 1-4 de l'assistant Decommission site si un ou plusieurs nœuds sont déconnectés. Toutefois, vous ne pouvez pas effectuer l'étape 5 de l'assistant, qui démarre le processus de mise hors service, sauf si tous les nœuds sont connectés.

- Si le site que vous souhaitez supprimer contient un nœud de passerelle ou un nœud d'administration utilisé pour l'équilibrage de charge, vous devrez peut-être "développez une grille"ajouter un nouveau nœud équivalent sur un autre site. Assurez-vous que les clients peuvent vous connecter au nœud de remplacement avant de lancer la procédure de mise hors service du site.
- Si le site que vous prévoyez de supprimer contient un nœud de passerelle ou des nœuds d'administration qui se trouvent dans un groupe haute disponibilité, vous pouvez effectuer les étapes 1-4 de l'assistant dédié au site de mise hors service. Toutefois, vous ne pouvez pas effectuer l'étape 5 de l'assistant, qui démarre le processus de mise hors service, tant que vous n'avez pas supprimé ces nœuds de tous les groupes haute disponibilité. Si des clients existants se connectent à un groupe haute disponibilité incluant des nœuds du site, assurez-vous qu'ils peuvent continuer à se connecter à StorageGRID une fois le site supprimé.
- Si les clients se connectent directement aux nœuds de stockage du site que vous prévoyez de supprimer, assurez-vous qu'ils peuvent se connecter aux nœuds de stockage sur d'autres sites avant de lancer la procédure de mise hors service du site.
- Vous devez fournir suffisamment d'espace sur les sites restants pour prendre en charge toutes les données d'objet qui seront déplacées à cause des modifications apportées à une règle ILM active. Dans certains cas, vous devrez peut-être "développez une grille"ajouter des nœuds de stockage, des volumes de stockage ou de nouveaux sites avant de pouvoir désaffecter un site connecté.
- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée. Les processus ILM d'StorageGRID peuvent prendre plusieurs jours, semaines, voire plusieurs mois pour

déplacer ou supprimer les données d'objet depuis le site avant la mise hors service du site.



Le déplacement ou la suppression de données d'objet depuis un site peut prendre plusieurs jours, semaines, voire mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences réseau et de la nature des modifications ILM requises.

- Dans la mesure du possible, vous devez exécuter les étapes 1-4 de l'assistant Decommission site dès que possible. La procédure de mise hors service se termine plus rapidement et avec moins d'interruptions et d'impacts sur les performances si vous permettez le déplacement des données depuis le site avant de démarrer la procédure de mise hors service réelle (en sélectionnant **Démarrer la mise hors service** à l'étape 5 de l'assistant).

Exigences supplémentaires relatives à la mise hors service d'un site déconnecté

Avant que StorageGRID puisse supprimer un site déconnecté, vous devez vérifier ce qui suit :

- Vous avez contacté votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site.



N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer des données objet à partir du site. Voir "[Comment le support technique récupère un site](#)".

- Tous les nœuds du site doivent avoir un état de connexion de l'un des éléments suivants :
 - **Inconnu** (🌀) : Pour une raison inconnue, un nœud est déconnecté ou les services 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 interruption inattendue.
 - **Hors service administrativement** (🌙) : Le nœud n'est pas connecté à la grille pour une raison prévue. 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 consulter ou récupérer toutes les données d'objet qui ont été stockées sur le site. Lorsque StorageGRID exécute cette procédure, il ne tente pas de préserver les données du site déconnecté.



Si vos règles et règles ILM ont été conçues pour protéger contre la perte d'un seul site, des copies de vos objets existent toujours sur les sites restants.

- Vous devez comprendre que si le site contenait la seule copie d'un objet, l'objet est perdu et ne peut pas être récupéré.

Considérations de cohérence lorsque vous supprimez un site

La cohérence d'un compartiment S3 détermine si StorageGRID réplique entièrement les métadonnées d'objet sur tous les nœuds et sites avant de dire à un client que l'ingestion d'objet a abouti. La cohérence assure un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites.

Lorsque StorageGRID supprime un site, il doit s'assurer qu'aucune donnée n'est écrite sur le site supprimé.

Par conséquent, elle remplace temporairement la cohérence de chaque compartiment ou conteneur. Une fois le processus de mise hors service du site démarré, StorageGRID utilise temporairement une cohérence forte entre les sites pour empêcher l'écriture des métadonnées d'objet sur le site.

Par conséquent, sachez que toute opération d'écriture, de mise à jour et de suppression du client qui se produit lors de la désaffectation d'un site peut échouer si plusieurs nœuds ne sont plus disponibles sur les sites restants.

Rassemblez les matériaux nécessaires pour la mise hors service du site StorageGRID

Avant de mettre un site hors service, vous devez obtenir les documents suivants.

Élément	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 de package de récupération pour restaurer le système en cas de panne. "Téléchargez le package de récupération"
Passwords.txt fichier	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.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement ne se trouve pas dans Passwords.txt le fichier.
Description de la topologie du système StorageGRID avant la mise hors service	Le cas échéant, procurez-vous toute documentation décrivant la topologie actuelle du système.

Informations associées

["Navigateurs Web pris en charge"](#)

Sélectionnez un site à mettre hors service dans StorageGRID

Pour déterminer si un site peut être déclassé, commencez par accéder à l'assistant Decommission site.

Avant de commencer

- Vous avez obtenu tous les matériaux requis.
- Vous avez examiné les considérations relatives à la suppression d'un site.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["L'autorisation d'accès racine ou les autorisations Maintenance et ILM"](#).

Étapes

1. Sélectionnez **Maintenance > Tâches > Mise hors service**.

2. Sélectionnez **site de désaffectation**.

L'étape 1 (Sélectionner le site) de l'assistant de site de désaffectation s'affiche. Cette étape contient 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

3. Affichez les valeurs de la colonne capacité de stockage * utilisée pour déterminer la quantité de stockage actuellement utilisée pour les données d'objet de chaque site.

La capacité de stockage utilisée est une estimation. Si les nœuds sont hors ligne, la capacité de stockage utilisée est la dernière valeur connue du site.

- Dans le cas d'une désaffectation d'un site connecté, cette valeur représente la quantité de données d'objet à déplacer vers d'autres sites ou à supprimer via ILM avant de désaffecter ce site en toute sécurité.
- Dans le cas d'une désaffectation de site déconnectée, cette valeur représente la proportion de stockage de données de votre système qui deviendra inaccessible lorsque vous désaffectez ce site.



Si votre politique ILM a été conçue pour vous protéger contre la perte d'un seul site, des copies de vos données d'objet doivent toujours exister sur les sites restants.

4. Consultez les raisons de la colonne **Decommission possible** pour déterminer quels sites peuvent être désaffectés actuellement.



S'il y a plusieurs raisons pour lesquelles un site ne peut pas être désaffecté, la raison la plus critique est indiquée.

Motif de mise hors service possible	Description	Étape suivante
Coche verte (✓)	Vous pouvez désaffecter ce site.	Allez à l'étape suivante.
Non. Ce site contient le nœud d'administration principal.	Vous ne pouvez pas désaffecter un site contenant le nœud d'administration principal.	Aucune. Vous ne pouvez pas effectuer cette procédure.
Non. Ce site contient un ou plusieurs nœuds d'archivage.	Vous ne pouvez pas désaffecter un site contenant un nœud d'archivage.	Aucune. Vous ne pouvez pas effectuer cette procédure.
Non. Tous les nœuds de ce site sont déconnectés. Contactez votre ingénieur commercial NetApp.	Vous ne pouvez pas effectuer la mise hors service d'un site connecté à moins que chaque nœud du site ne soit connecté (✓).	Si vous souhaitez effectuer une mise hors service hors site déconnectée, vous devez contacter votre ingénieur commercial NetApp, qui examinera vos besoins et active le reste de l'assistant de mise hors service. IMPORTANT: Ne mettez jamais les noeuds en ligne hors ligne pour que vous puissiez supprimer un site. Vous allez perdre des données.

L'exemple illustre un système StorageGRID avec trois sites. La coche verte (✓) pour les sites de Raleigh et Sunnyvale indique que vous pouvez mettre ces sites hors service. Cependant, vous ne pouvez pas mettre le site de Vancouver hors service car il contient le nœud d'administration principal.

1. Si une mise hors service est possible, sélectionnez le bouton radio du site.

Le bouton **Suivant** est activé.

2. Sélectionnez **Suivant**.

L'étape 2 (Détails de la vue) s'affiche.

Consultez les détails du site avant la mise hors service dans StorageGRID

À partir de l'étape 2 (Afficher les détails) de l'assistant Decommission site, vous pouvez vérifier quels nœuds sont inclus sur le site, voir combien d'espace a été utilisé sur chaque nœud de stockage et évaluer la quantité d'espace disponible sur les autres sites de votre grille.

Avant de commencer

Avant de désaffecter un site, vous devez vérifier la quantité de données d'objet présentes sur le site.

- Si vous effectuez une mise hors service d'un site connecté, vous devez connaître la quantité de données d'objet présentes sur le site avant de mettre à jour le ILM. En fonction des capacités de votre site et de vos besoins en termes de protection des données, vous pouvez créer de nouvelles règles ILM pour déplacer des données vers d'autres sites ou supprimer les données d'objet du site.
- Exécutez les extensions du nœud de stockage requises avant de démarrer la procédure de mise hors service si possible.
- Si vous effectuez une mise hors service de site déconnecté, vous devez comprendre combien de données d'objet deviennent définitivement inaccessibles lorsque vous supprimez le site.

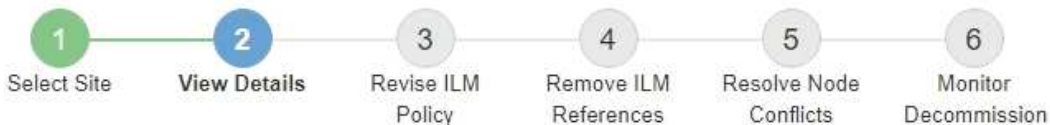


Si vous désaffectez un site, la règle ILM ne permet pas de déplacer ou de supprimer des données d'objet. Toutes les données conservées sur le site seront perdues. Toutefois, si votre politique ILM a été conçue pour protéger contre la perte d'un seul site, des copies de vos données d'objet existent toujours sur les sites restants. Voir "[Activer la protection contre la perte de site](#)".

Étapes

1. À partir de l'étape 2 (Afficher les détails), passez en revue tous les avertissements relatifs au site que vous avez sélectionné pour le supprimer.

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.

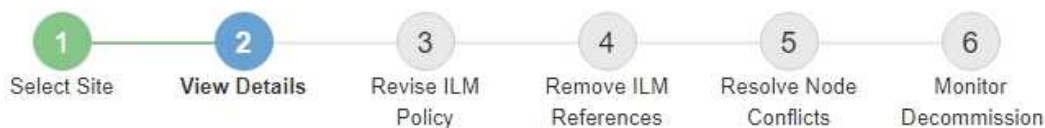
This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

Un avertissement apparaît dans ces cas :

- Le site inclut un nœud de passerelle. Si les 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 nœuds connectés () et de nœuds déconnectés (ou). Avant de pouvoir supprimer ce site, vous devez remettre en ligne tous les nœuds hors ligne.

2. Examinez les détails du site que vous avez sélectionné pour le 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
- Espace utilisé total, espace libre et capacité de tous les nœuds de stockage du site.
 - Pour une mise hors service de site connecté, la valeur **espace utilisé** représente la quantité de données d'objet à déplacer vers d'autres sites ou à supprimer avec ILM.
 - Pour une mise hors service du site déconnecté, la valeur **espace utilisé** indique la quantité de données d'objet qui deviennent inaccessibles lorsque vous supprimez le site.
- Noms, types et États de connexion des nœuds :
 -  (Connecté)
 -  (Administrativement désactivé)
 -  (Inconnu)
- Détails sur chaque nœud :
 - Pour chaque nœud de stockage, quantité d'espace utilisée pour les données d'objet.

- Pour les nœuds d'administration et les nœuds de passerelle, que le nœud soit actuellement utilisé dans un groupe haute disponibilité (HA). Vous ne pouvez pas désaffecter un nœud d'administration ou un nœud de passerelle utilisé dans un groupe haute disponibilité. Avant de commencer la désaffectation, éditez les groupes haute disponibilité pour supprimer tous les nœuds du site ou supprimez le groupe haute disponibilité si seuls les nœuds sont inclus dans ce site. Pour obtenir des instructions, reportez-vous à la section "[Gestion des groupes haute disponibilité](#)".

3. Dans la section Détails des autres sites de la page, évaluez la quantité d'espace disponible sur les autres sites de votre grille.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB

Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Si vous désaffectez un site connecté et que vous prévoyez d'utiliser ILM pour déplacer les données d'objet depuis le site sélectionné (au lieu de simplement les supprimer), vous devez vous assurer que les autres sites disposent de la capacité suffisante pour prendre en charge les données déplacées et que la capacité adéquate reste adaptée à la croissance future.



Un avertissement s'affiche si l'espace **utilisé** pour le site que vous souhaitez supprimer est supérieur à **l'espace libre total pour les autres sites**. Pour garantir que la capacité de stockage adéquate est disponible après le retrait du site, vous devrez peut-être procéder à une extension avant d'effectuer cette procédure.

4. Sélectionnez **Suivant**.

L'étape 3 (réviser la politique ILM) s'affiche.

Réviser les politiques ILM pour la mise hors service de site dans StorageGRID

A partir de l'étape 3 (réviser les règles ILM) de l'assistant site de désaffectation, vous pouvez déterminer si le site est référencé par une stratégie ILM.

Avant de commencer

Vous avez une bonne compréhension de "[Gestion des objets avec la solution ILM](#)" la façon de . Vous connaissez déjà la création de pools de stockage et de règles ILM, ainsi que la simulation et l'activation d'une stratégie ILM.

Description de la tâche

StorageGRID ne peut pas désaffecter un site si une règle ILM dans n'importe quelle règle (active ou inactive) fait référence à ce site.

Si une règle ILM fait référence au site que vous souhaitez désaffecter, vous devez supprimer ces règles ou les modifier pour qu'elles répondent aux exigences suivantes :

- Protégez intégralement toutes les données d'objet.
- Ne faites pas référence au site que vous êtes en train de désaffecter.
- N'utilisez pas de pools de stockage faisant référence au site ou l'option tous les sites.
- N'utilisez pas les profils de code d'effacement qui font référence au site.
- N'utilisez pas la règle Make 2 copies à partir d'installations StorageGRID 11.6 ou antérieures.



Ne créez jamais de règle ILM à copie unique pour la suppression d'un site. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.



Si vous effectuez une *désaffectation de site connecté*, vous devez tenir compte de la manière dont StorageGRID doit gérer les données d'objet actuellement sur le site que vous souhaitez supprimer. Selon vos exigences en matière de protection des données, de nouvelles règles peuvent déplacer les données d'objet existantes vers d'autres sites ou supprimer toute copie d'objet supplémentaire qui n'est plus nécessaire.

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 règles ILM), déterminez si des règles ILM font référence au site que vous avez choisi de désaffecter.
2. Si aucune stratégie n'est répertoriée, sélectionnez **Suivant** pour accéder à ["Étape 4 : supprimer les références ILM"](#).
3. Si une ou plusieurs règles ILM *active* sont répertoriées, clonez chaque règle existante ou créez de nouvelles règles qui ne référencent pas le site mis hors service :
 - a. Sélectionnez le lien de la règle dans la colonne Nom de la règle.

La page de détails de la politique ILM s'affiche dans un nouvel onglet de navigateur. La page site de désaffectation reste ouverte dans l'onglet autre.

- b. Suivez les directives et instructions suivantes si nécessaire :

- Utilisation des règles ILM :
 - ["Créez un ou plusieurs pools de stockage"](#) qui ne font pas référence au site.
 - ["Modifier ou remplacer des règles"](#) qui se rapportent au site.



Ne sélectionnez pas la règle **make 2 copies** car cette règle utilise le pool de stockage **All Storage Nodes**, qui n'est pas autorisé.

- Utilisation des règles ILM :
 - ["Cloner une règle ILM existante"](#) ou ["Création d'une règle 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 l'ordre correct. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut.

c. Ingérer des objets de test et simuler la règle pour s'assurer que les règles correctes sont appliquées.



Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

d. Activez les nouvelles stratégies et assurez-vous que les anciennes sont inactives.

Si vous souhaitez activer plusieurs stratégies, "[Suivez la procédure de création des balises de règles ILM](#)".

Si vous effectuez une mise hors service du site connecté, StorageGRID commence à supprimer les données d'objet du site sélectionné dès que vous activez la nouvelle règle ILM. Le déplacement ou la suppression de toutes les copies d'objet peut prendre plusieurs semaines. Vous pouvez démarrer en toute sécurité une mise hors service d'un site alors que les données d'objet existent toujours sur le site. Toutefois, la procédure de mise hors service est plus rapide et avec moins de perturbations et d'impacts sur les performances si vous permet de déplacer les données depuis le site avant de démarrer la procédure de mise hors service (En sélectionnant **Start Decommission** à l'étape 5 de l'assistant).

4. Pour chaque règle *inactive*, modifiez-la ou supprimez-la en sélectionnant d'abord le lien de chaque règle comme décrit dans les étapes précédentes.
 - "[Modifiez la stratégie](#)" il ne fait donc pas référence au site à mettre hors service.
 - "[Supprimer une stratégie](#)".
5. Lorsque vous avez terminé d'apporter des modifications aux règles et règles ILM, plus aucune règle ne doit être répertoriée à l'étape 3 (réviser les règles ILM). Sélectionnez **Suivant**.

L'étape 4 (Supprimer les références ILM) s'affiche.

Supprimer les références ILM à un site dans StorageGRID

À partir de l'étape 4 (Supprimer les références ILM) de l'assistant site de désaffectation, vous devez supprimer ou modifier toutes les règles ILM inutilisées qui font référence au site, même si ces règles ne sont pas utilisées dans une stratégie ILM.

Étapes

1. Déterminez si des règles ILM inutilisées font référence au site.

Si des règles ILM sont répertoriées, elles font toujours référence au site, mais ne sont utilisées dans aucune règle.



Lorsque StorageGRID décompresse le site, il désactive automatiquement les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Le pool de stockage tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) est supprimé car il utilise le site tous les sites.

2. Modifier ou supprimer chaque règle inutilisée :

- Pour modifier une règle, accédez à la page de règles ILM et mettez à jour tous les placements qui utilisent un profil de code d'effacement ou un pool de stockage faisant référence au site. Ensuite, revenez à **étape 4 (Supprimer les références ILM)**.
- Pour supprimer une règle, sélectionnez l'icône de la corbeille  et sélectionnez **OK**.



Vous devez supprimer la règle **make 2 copies** avant de pouvoir désaffecter un site.

3. Vérifiez qu'aucune règle ILM inutilisée ne fait référence au site et que le bouton **Suivant** est activé.

4. Sélectionnez **Suivant**.



Les pools de stockage et les profils de code d'effacement qui font référence au site ne seront plus valides après la suppression du site. Lorsque StorageGRID décompresse le site, il désactive automatiquement les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Le pool de stockage tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) est supprimé car il utilise le site tous les sites.

L'étape 5 (résoudre les conflits de nœuds) s'affiche.

Résolvez les conflits de nœuds et démarrez la mise hors service du site dans StorageGRID

À partir de l'étape 5 (résoudre les conflits de nœuds) de l'assistant site de mise hors service, vous pouvez déterminer si des nœuds de votre système StorageGRID sont déconnectés ou si des nœuds du site sélectionné appartiennent à un groupe haute disponibilité (HA). Après la résolution d'un conflit de nœud, vous démarrez la procédure de mise hors service à partir de cette page.

Avant de commencer

Vous devez vous assurer que tous les nœuds de votre système StorageGRID sont dans l'état approprié, comme suit :

- Tous les nœuds de votre système StorageGRID doivent être connectés (.



Si vous effectuez une mise hors service du site déconnecté, tous les nœuds du site que vous supprimez doivent être déconnectés et tous les nœuds de tous les autres sites doivent être connectés.



La mise hors service ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.



Si un ou plusieurs volumes sont déconnectés alors qu'une mise hors service est en cours, le processus de mise hors service se termine une fois ces volumes remis en ligne.

- Aucun nœud sur le site que vous supprimez peut avoir une interface appartenant à un groupe haute disponibilité.

Description de la tâche

Si un nœud est répertorié pour l'étape 5 (résoudre les conflits de nœud), vous devez corriger le problème avant de pouvoir démarrer la mise hors service.

Avant de commencer la procédure de mise hors service du site à partir de cette page, prenez en compte les considérations suivantes :

- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée.



Le déplacement ou la suppression de données d'objet depuis un site peut prendre plusieurs jours, semaines, voire mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences réseau et de la nature des modifications ILM requises.

- Pendant que la procédure de mise hors service du site est en cours d'exécution :
 - Vous ne pouvez pas créer de règles ILM faisant référence au site en cours de désaffectation. Vous ne pouvez pas non plus modifier une règle ILM existante pour faire référence au site.
 - Vous ne pouvez pas effectuer d'autres procédures de maintenance, telles que l'extension ou la mise à niveau.



Si vous devez effectuer une autre procédure de maintenance lors de la mise hors service d'un site connecté, vous pouvez interrompre la procédure pendant que les nœuds de stockage sont supprimés. Le bouton **Pause** est activé pendant l'étape "données répliquées et codées d'effacement de la désaffectation".

- Si vous devez récupérer un nœud après avoir lancé la procédure de mise hors service du site, vous devez contacter le service de support.

Étapes

1. 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 hors service ()

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 un nœud est déconnecté, remettre en ligne.

Voir la "[Procédures de nœud](#)". Contactez le support technique si vous avez besoin d'aide.

3. Lorsque tous les nœuds déconnectés ont été remis en ligne, passez en revue la section HA Groups de l'étape 5 (résoudre les conflits de nœuds).

Ce tableau répertorie tous les nœuds du site sélectionné qui appartiennent à un groupe haute disponibilité (HA).

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 haute disponibilité affecté afin de supprimer l'interface de nœud.
- Supprimez un groupe haute disponibilité qui inclut uniquement les nœuds de ce site. Voir les instructions d'administration de StorageGRID.

Si tous les nœuds sont connectés et qu'aucun nœud du site sélectionné n'est utilisé dans un groupe HA, le champ **Provisioning passphrase** est activé.

5. Saisissez la phrase secrète pour le provisionnement.

Le bouton **Start Decommission** 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 mise hors service du site, sélectionnez **Start Decommission**.

Un avertissement répertorie le site et les nœuds qui seront supprimés. Nous vous rappelons qu'il peut prendre des jours, des semaines, voire des mois pour supprimer complètement le site.

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. Vérifiez l'avertissement. Si vous êtes prêt à commencer, sélectionnez **OK**.

Un message apparaît au fur et à mesure que la nouvelle configuration de grille est générée. Ce processus peut prendre un certain temps, selon le type et le nombre de nœuds de la grille désaffectés.

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 

Lorsque la nouvelle configuration de grille a été générée, l'étape 6 (Monitor Decommission) s'affiche.



Le bouton **Previous** reste désactivé jusqu'à ce que la mise hors service soit terminée.

Surveillez la progression de la mise hors service du site dans StorageGRID

À partir de l'étape 6 (Monitor Decommission) de l'assistant de page site de désaffectation, vous pouvez surveiller la progression du site à mesure que celui-ci est supprimé.

Description de la tâche

Lorsque StorageGRID supprime un site connecté, il supprime des nœuds dans l'ordre suivant :

1. Nœuds de passerelle
2. Nœuds d'administration
3. Nœuds de stockage

Lorsque StorageGRID supprime un site déconnecté, il supprime des nœuds dans l'ordre suivant :

1. Nœuds de passerelle
2. Nœuds de stockage
3. Nœuds d'administration

La suppression de chaque nœud de passerelle ou d'un nœud d'administration peut prendre quelques minutes ou une heure. En revanche, les nœuds de stockage peuvent prendre des jours ou des semaines.

Étapes

1. Dès qu'un nouveau package de récupération a été généré, téléchargez le fichier.

Decommission Site



i 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 fichier.

Voir les instructions pour "[téléchargement du package de récupération](#)".

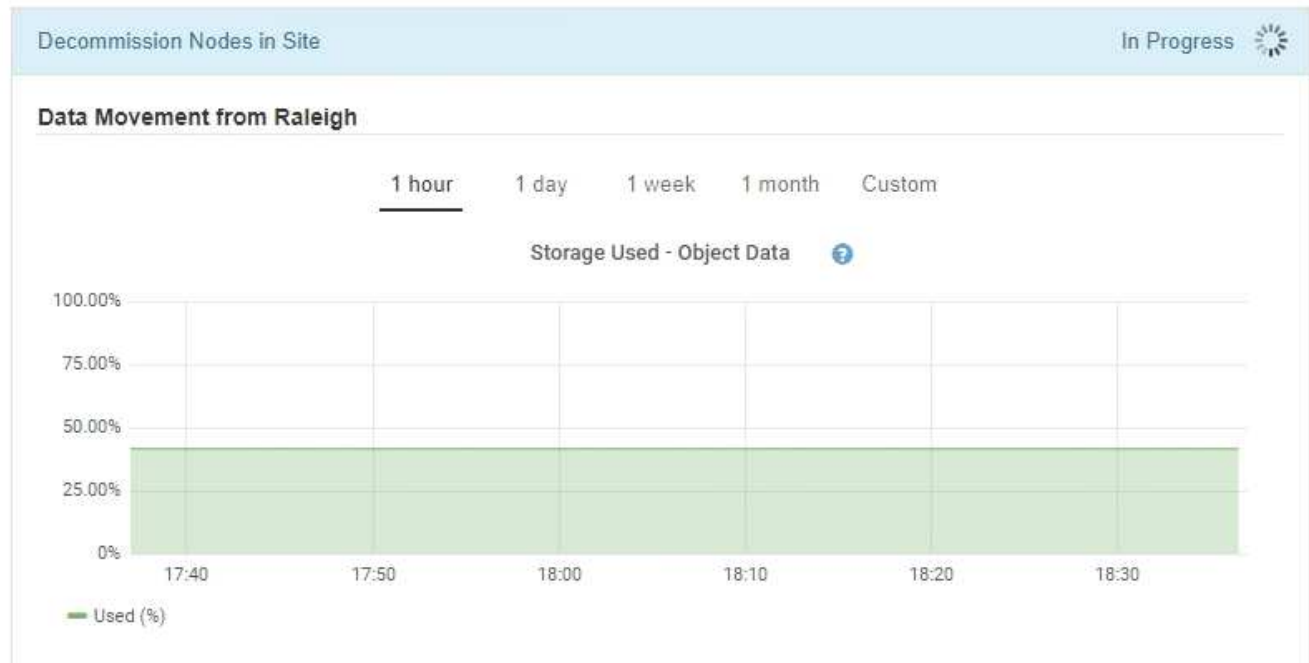


Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

2. À l'aide du diagramme de déplacement des données, surveillez le déplacement des données d'objet de ce site vers d'autres sites.

Le déplacement des données a commencé lorsque vous avez activé la nouvelle règle ILM à l'étape 3 (réviser la politique ILM). Un déplacement des données sera effectué tout au long de la procédure de mise hors service.

Decommission Site Progress



3. Dans la section progression du nœud de la page, surveillez la progression de la procédure de mise hors service lorsque les nœuds sont supprimés.

Lorsqu'un nœud de stockage est supprimé, chaque nœud passe par une série d'étapes. Si la plupart de ces étapes se produisent rapidement, voire de façon imperceptible, vous devrez peut-être attendre des jours, voire des semaines, pour les autres étapes, et déterminer le volume de données à déplacer. Du temps supplémentaire est nécessaire pour gérer les données codées et réévaluer les règles ILM.

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

Search 					
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 désaffectation d'un site connecté, consultez ce tableau pour comprendre les étapes de mise hors service d'un nœud de stockage :

Étape	Durée estimée
En attente	Minute ou moins
Attendez les verrous	Quelques minutes
Préparer la tâche	Minute ou moins
Marquage LDR déclassé	Quelques minutes
Déclassement des données répliquées et des données avec code d'effacement	Heures, jours ou semaines en fonction de la quantité de données Remarque : si vous devez effectuer d'autres activités de maintenance, vous pouvez mettre le site hors service pendant cette étape.
Etat défini LDR	Quelques minutes
Vider les files d'attente d'audit	Quelques minutes à plusieurs heures, selon le nombre de messages et la latence du réseau.
Terminé	Quelques minutes

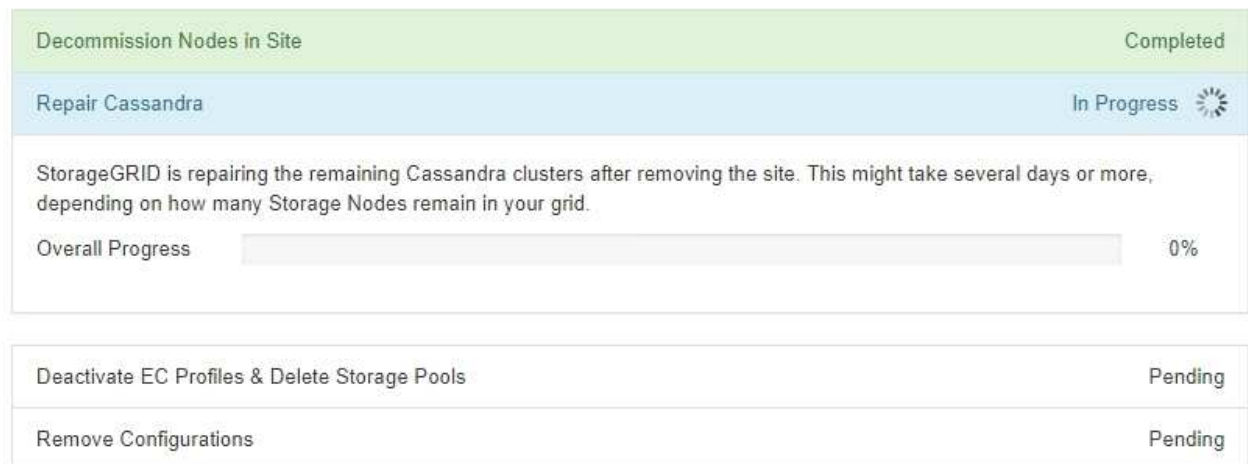
Si vous surveillez la progression d'une mise hors service d'un site déconnecté, consultez ce tableau pour connaître les étapes de mise hors service d'un nœud de stockage :

Étape	Durée estimée
En attente	Minute ou moins
Attendez les verrous	Quelques minutes
Préparer la tâche	Minute ou moins
Désactiver les services externes	Quelques minutes
Révocation de certificat	Quelques minutes
Annulation de l'enregistrement du nœud	Quelques minutes
Annulation du registre de notes de stockage	Quelques minutes
Retrait du groupe de stockage	Quelques minutes

Étape	Durée estimée
Suppression d'entité	Quelques minutes
Terminé	Quelques minutes

4. Une fois que tous les nœuds ont atteint l'étape terminée, attendez la fin des opérations de désaffectation du site restantes.
 - Pendant l'étape **réparer Cassandra**, StorageGRID effectue les réparations nécessaires aux clusters Cassandra qui restent dans votre réseau. Ces réparations peuvent prendre plusieurs jours ou plus, selon le nombre de nœuds de stockage restants dans votre grid.

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 code d'effacement faisant référence au site sont désactivés.
 - Tous les pools de stockage auxquels le site fait référence sont supprimés.



Le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) est également supprimé car il utilise le site tous les sites.

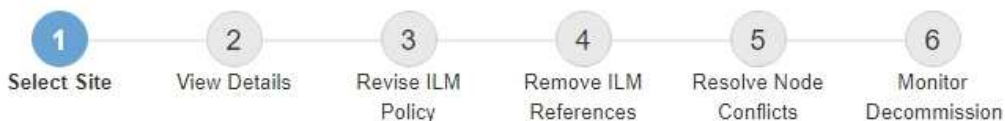
- Enfin, lors de l'étape **Remove Configuration**, toutes les références restantes au site et à ses nœuds sont supprimées du reste de la grille.

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

Une fois que vous avez terminé

Effectuez les tâches suivantes une fois la procédure de mise hors service du site terminée :

- Assurez-vous que les disques de tous les nœuds de stockage du site mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.
- Si le site inclut un ou plusieurs nœuds d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, supprimez toutes les approbations de tiers de confiance pour le site de Active Directory Federation Services (AD FS).
- Une fois que les nœuds ont été mis hors tension automatiquement dans le cadre de la procédure de mise

hors service du site connecté, supprimez les machines virtuelles associées.

Renommez la grille, le site ou le nœud

Utilisez la procédure de renommage StorageGRID

Si nécessaire, vous pouvez modifier les noms d’affichage affichés dans le Gestionnaire de grille pour l’ensemble de la grille, chaque site et chaque nœud. Vous pouvez mettre à jour les noms d’affichage en toute sécurité et à tout moment.

Qu’est-ce que la procédure de renommage ?

Lorsque vous installez StorageGRID au départ, vous spécifiez un nom pour la grille, chaque site et chaque nœud. Ces noms initiaux sont connus sous le nom de *System Names*, et ils sont les noms initialement affichés dans StorageGRID.

Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés. Toutefois, vous pouvez utiliser la procédure rename pour définir de nouveaux *noms d’affichage* pour la grille, chaque site et chaque nœud. Ces noms d’affichage apparaissent dans divers emplacements StorageGRID au lieu (ou dans certains cas, en plus de) des noms de système sous-jacents.

Utilisez la procédure de renommage pour corriger les fautes de frappe, mettre en œuvre une convention de nommage différente ou indiquer qu’un site et tous ses nœuds ont été déplacés. Contrairement aux noms des systèmes, les noms d’affichage peuvent être mis à jour en fonction des besoins et sans incidence sur les opérations StorageGRID.

Où les noms du système et de l’affichage apparaissent-ils ?

Le tableau suivant récapitule les emplacements où les noms des systèmes et les noms d’affichage sont affichés dans l’interface utilisateur de StorageGRID et dans les fichiers StorageGRID.

Emplacement	Nom du système	Nom d'affichage
Pages Grid Manager	Affiché sauf si l'élément est renommé	Si un élément est renommé, affiché à la place du nom du système dans les emplacements suivants : • Tableau de bord • Page nœuds • Pages de configuration pour les groupes haute disponibilité, les terminaux d'équilibrage de charge, les interfaces VLAN, les serveurs de gestion des clés, les mots de passe grid, et le contrôle du pare-feu • Alertes • Définitions de pool de stockage • Page de recherche de métadonnées d'objet • Pages relatives aux procédures de maintenance, y compris la mise à niveau, le correctif, la mise à niveau du système d'exploitation SANtricity, la mise hors service, expansion, récupération et vérification de l'existence de l'objet • Pages de support (journaux et diagnostics) • Page d'ouverture de session unique, en regard du nom d'hôte du nœud d'administration dans le tableau pour les détails du nœud d'administration
Nœuds > onglet Aperçu pour un nœud	Toujours affiché	S'affiche uniquement si l'élément est renommé
API Node-Health	Toujours renvoyé	Renvoyé uniquement si l'élément est renommé
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>

Emplacement	Nom du système	Nom d’affichage
`Passwords.txt` fichier dans le package de récupération	Comme illustré Server Name	Comme illustré Display Name
/etc/hosts sur tous les nœuds Par exemple : 10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host	Toujours affiché dans la deuxième colonne	Lorsque l’élément est renommé, il apparaît dans la quatrième colonne
topology-display-names.json, Inclus avec les données AutoSupport	Non inclus	Vide, sauf si les éléments ont été renommés ; sinon, mappe les ID de grille, de site et de nœud sur leurs noms d’affichage.

Afficher les exigences relatives au nom

Avant d'utiliser cette procédure, vérifiez les exigences relatives aux noms d’affichage.

Afficher les noms des nœuds

Les noms d’affichage des nœuds doivent respecter les règles suivantes :

- Doit être unique sur l’ensemble de votre système StorageGRID.
- Ne peut pas être identique au nom système d’un autre élément de votre système StorageGRID.
- Doit contenir au moins 1 et 32 caractères.
- Peut contenir des chiffres, des tirets (-) et des lettres majuscules et minuscules.
- Peut commencer ou se terminer par une lettre ou un chiffre, mais ne peut pas commencer ou se terminer par un tiret.
- Ne peut pas être tous des nombres.
- Ne sont pas sensibles à la casse. Par exemple, DC1-ADM et dc1-adm sont considérés comme des doublons.

Vous pouvez renommer un nœud avec un nom d’affichage précédemment utilisé par un autre nœud, à condition que le renommage ne crée pas de nom d’affichage ni de nom de système en double.

Afficher les noms de la grille et des sites

Les noms d’affichage de la grille et des sites suivent les mêmes règles avec les exceptions suivantes :

- Peut inclure des espaces.
- Les caractères spéciaux suivants peuvent être inclus : = - _ : , . @ !
- Vous pouvez commencer et terminer par les caractères spéciaux, y compris les tirets.
- Il peut s’agir de tous les chiffres ou de caractères spéciaux.

Meilleures pratiques relatives aux noms d’affichage

Si vous prévoyez de renommer plusieurs éléments, documentez votre schéma de dénomination général avant d’utiliser cette procédure. Trouvez un système qui garantit que les noms sont uniques, cohérents et faciles à comprendre d’un seul coup d’œil.

Vous pouvez utiliser n’importe quelle convention de dénomination adaptée aux besoins de votre entreprise. Prenez en compte les suggestions de base suivantes concernant les éléments à inclure :

- **Indicateur de site** : si vous avez plusieurs sites, ajoutez un code de site à chaque nom de nœud.
- **Type de nœud** : les noms de nœud 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 deux fois avant d’ajouter des détails spécifiques aux noms susceptibles de changer au fil du temps. Par exemple, n’incluez pas d’adresses IP dans les noms de nœuds car ces adresses peuvent être modifiées. De même, l’emplacement des racks ou les numéros de modèle des appliances peuvent changer si vous déplacez des équipements ou mettez à niveau le matériel.

Exemples de noms d’affichage

Supposons que votre système StorageGRID dispose de trois data centers et que chaque data Center dispose de nœuds de différents types. Vos noms d’affichage peuvent être aussi simples que ceux-ci :

- **Grille** : StorageGRID Deployment
- **Premier site** : Data Center 1
 - `dc1-adm1`
 - `dc1-s1`
 - `dc1-s2`
 - `dc1-s3`
 - `dc1-gw1`
- **Deuxième site** : Data Center 2
 - `dc2-adm2`
 - `dc2-s1`
 - `dc2-s2`

- dc2-s3

- **Troisième site:** Data Center 3

- dc3-s1

- dc3-s2

- dc3-s3

Ajouter ou mettre à jour les noms d’affichage StorageGRID

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 de n’importe quel nœud d’administration, vous êtes connecté au gestionnaire de grille à l’aide d’un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d’accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous comprenez les exigences et les meilleures pratiques en matière d’affichage des noms. Voir ["Renommez la grille, les sites et les nœuds"](#).

Comment renommer la grille, les sites ou les nœuds

Vous pouvez renommer votre système StorageGRID, un ou plusieurs sites ou un ou plusieurs nœuds.

Vous pouvez utiliser un nom d’affichage précédemment utilisé par un autre nœud, tant que le changement de nom n’entraîne pas de doublon de nom d’affichage ou de nom de système.

Sélectionnez les éléments à renommer

Pour commencer, sélectionnez les éléments à renommer.

Étapes

1. Sélectionnez **Maintenance > Tâches > Renommer la grille, les sites et les nœuds**.
2. Pour l’étape **Sélectionner les noms**, sélectionnez les éléments que vous souhaitez renommer.

Élément à modifier	Instructions
Noms de tout (ou presque tout) dans votre système	a. Sélectionnez Sélectionner tout . b. Vous pouvez également effacer les éléments que vous ne souhaitez pas renommer.
Nom de la grille	Cochez la case de la grille.

Élément à modifier	Instructions
Nom d'un site et de certains ou de tous ses nœuds	a. Cochez la case dans l'en-tête du tableau pour le site. b. Si vous le souhaitez, désactivez les nœuds que vous ne souhaitez pas renommer.
Nom d'un site	Cochez la case du site.
Nom d'un nœud	Cochez la case du nœud.

3. Sélectionnez **Continuer**.

4. Passez en revue le tableau, qui inclut les éléments que vous avez sélectionnés.

- La colonne **Nom d'affichage** indique le nom actuel de chaque élément. Si l'élément n'a jamais été renommé, son nom d'affichage est le même que son nom système.
- La colonne **Nom du système** indique le nom que vous avez saisi pour chaque élément au cours de l'installation. Les noms de système sont utilisés pour les opérations StorageGRID internes et ne peuvent pas être modifiés. Par exemple, le nom système d'un nœud peut correspondre à son nom d'hôte.
- La colonne **Type** indique le type de l'élément : grille, site ou le type de nœud spécifique.

Proposer de nouveaux noms

Pour l'étape **proposer de nouveaux noms**, vous pouvez entrer un nom d'affichage pour chaque élément individuellement ou renommer les éléments en bloc.

Renommer les éléments individuellement

Procédez comme suit pour entrer un nom d’affichage pour chaque élément à renommer.

Étapes

1. Dans le champ **Nom d’affichage**, entrez un nom d’affichage proposé pour chaque élément de la liste.

Reportez-vous à la section "[Renommez la grille, les sites et les nœuds](#)" pour connaître les exigences de nommage.

2. Pour supprimer les éléments que vous ne souhaitez pas renommer, sélectionnez  dans la colonne **Supprimer de la liste**.

Si vous ne proposez pas de nouveau nom pour un élément, vous devez le supprimer de la table.

3. Lorsque vous avez proposé de nouveaux noms pour tous les éléments de la table, sélectionnez **Renommer**.

Un message de réussite s’affiche. Les nouveaux noms d’affichage sont maintenant utilisés dans le Gestionnaire de grille.

Renommer les éléments en bloc

Utilisez l’outil de renommage en bloc si les noms d’élément partagent une chaîne commune que vous souhaitez remplacer par une autre chaîne.

Étapes

1. Pour l’étape **proposer de nouveaux noms**, sélectionnez **utiliser l’outil de renommage en bloc**.

L’aperçu **Renommer** inclut tous les éléments affichés pour l’étape **proposer de nouveaux noms**. Vous pouvez utiliser l’aperçu pour voir comment les noms d’affichage seront pris en compte après le remplacement d’une chaîne partagée.

2. Dans le champ **existing string**, entrez la chaîne partagée que vous souhaitez remplacer. Par exemple, si la chaîne que vous souhaitez remplacer est `Data-Center-1`, entrez **Data-Center-1**.

Au fur et à mesure que vous tapez, votre texte est mis en surbrillance à l’endroit où il se trouve dans les noms à gauche.

3. Sélectionnez  pour supprimer les éléments que vous ne souhaitez pas renommer avec cet outil.

Par exemple, supposons que vous souhaitiez renommer tous les nœuds contenant la chaîne `Data-Center-1`, mais que vous ne vouliez pas renommer le `Data-Center-1` site lui-même. Sélectionnez  pour retirer le site de l’aperçu du 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**, entrez la chaîne de remplacement que vous souhaitez utiliser. Par exemple, entrez **DC1**.

Reportez-vous à la section "[Renommez la grille, les sites et les nœuds](#)" pour connaître les exigences de nommage.

Lorsque vous entrez la chaîne de remplacement, les noms à gauche sont mis à jour, ce qui vous permet de vérifier que les nouveaux noms seront corrects.

1394

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 à la table pour l'étape **proposer de nouveaux noms**.
- Apportez les modifications supplémentaires nécessaires ou sélectionnez ✕ pour supprimer les éléments que vous ne souhaitez pas renommer.
- Lorsque vous êtes prêt à renommer tous les éléments de la table, sélectionnez **Renommer**.

Un message de réussite s'affiche. Les nouveaux noms d'affichage sont maintenant utilisés dans le Gestionnaire de grille.

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 pour le provisionnement.
- Sélectionnez **Télécharger le paquet de récupération**.

Le téléchargement commence immédiatement.

- Une fois le téléchargement terminé, ouvrez `Passwords.txt` le 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 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 du système StorageGRID.

5. Sélectionnez **Terminer** pour revenir à la première étape.

Rétablit les noms d’affichage des noms système

Vous pouvez rétablir le nom d’origine d’une grille, d’un site ou d’un nœud renommé. Lorsque vous rétablissez le nom système d’un élément, les pages du Gestionnaire de grille et les autres emplacements StorageGRID n’affichent plus de **Nom d’affichage** pour cet élément. Seul le nom système de l’élément est affiché.

Étapes

1. Sélectionnez **Maintenance > Tâches > Renommer la grille, les sites et les nœuds**.
2. Pour l’étape **Sélectionner les noms**, sélectionnez les éléments que vous souhaitez restaurer aux noms système.
3. Sélectionnez **Continuer**.
4. Pour l’étape **proposer de nouveaux noms**, restaurez les noms d’affichage individuellement ou en bloc.

Revenir aux noms de système individuellement

- a. Copiez le nom système d’origine de chaque élément et collez-le dans le champ **Nom d’affichage**, ou sélectionnez  pour supprimer les éléments que vous ne souhaitez pas rétablir.

Pour rétablir un nom d’affichage, le nom du système doit apparaître dans le champ **Nom d’affichage**, mais le nom n’est pas sensible à la casse.

- b. Sélectionnez **Renommer**.

Un message de réussite s’affiche. Les noms d’affichage de ces éléments ne sont plus utilisés.

Revenir aux noms de système en bloc

- a. Pour l’étape **proposer de nouveaux noms**, sélectionnez **utiliser l’outil de renommage en bloc**.
- b. Dans le champ **existing string**, entrez la chaîne de nom d’affichage que vous souhaitez remplacer.
- c. Dans le champ **Nouvelle chaîne**, entrez la chaîne de nom système que vous souhaitez utiliser.
- d. Sélectionnez **Ajouter des noms** pour ajouter les noms à la table pour l’étape **proposer de nouveaux noms**.
- e. Vérifiez que chaque entrée du champ **Nom d’affichage** correspond au nom du champ **Nom système**. Apportez les modifications nécessaires ou sélectionnez  pour supprimer les éléments que vous ne souhaitez pas rétablir.

Pour rétablir un nom d’affichage, le nom du système doit apparaître dans le champ **Nom d’affichage**, mais le nom n’est pas sensible à la casse.

- f. Sélectionnez **Renommer**.

Un message de réussite s’affiche. Les noms d’affichage de ces éléments ne sont plus utilisés.

5. Téléchargez et enregistrez un nouveau package de récupération .

Les noms d'affichage des éléments que vous avez restaurés ne sont plus inclus dans le `Passwords.txt` fichier.

Procédures de nœud

Procédures de maintenance des nœuds StorageGRID

Vous devrez peut-être effectuer des procédures de maintenance relatives à des nœuds de grid ou des services de nœud spécifiques.

Déplacer l'ADC

Le "Service ADC" est situé sur certains nœuds de stockage. Dans certaines circonstances de mise hors service et de conversion de nœud, vous devez déplacer le service ADC vers un autre nœud de stockage sur le même site.

Convertir un nœud de stockage en nœud de données uniquement

Vous pouvez convertir les nœuds de stockage qui ne contiennent pas le service ADC en nœuds de stockage de données uniquement.

Redémarrage, arrêt et mise sous tension du nœud

Ces procédures permettent de redémarrer un ou plusieurs nœuds, d'arrêter et de redémarrer des nœuds ou de mettre les nœuds hors tension et de les rallumer.

Remappage des ports

Vous pouvez utiliser les procédures de remap des ports pour supprimer les remappés de port d'un nœud, par exemple, si vous souhaitez configurer un point final d'équilibreur de charge à l'aide d'un port qui a été précédemment remappé.

Gestionnaire de serveur

Server Manager s'exécute sur chaque nœud de la grille pour superviser le démarrage et l'arrêt des services et pour s'assurer que les services rejoignent et quittent aisément le système StorageGRID. Server Manager surveille également les services sur chaque nœud de la grille et tente automatiquement de redémarrer les services qui signalent les pannes.

Pour exécuter les procédures du Gestionnaire de serveur, vous devez généralement accéder à la ligne de commande du nœud.



Vous ne devez accéder à Server Manager que si le support technique vous a demandé de le faire.

Déplacer le service ADC dans StorageGRID

Vous pouvez déplacer le service ADC vers un autre nœud de stockage sur le même site.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Tu as "Maintenance ou autorisation d'accès racine" .

- Le nœud source contient le service ADC.
- Le nœud cible ne contient pas le service ADC.
- Le nœud cible est soit un nœud contenant uniquement des métadonnées, soit un nœud combiné (métadonnées et données d'objet).
- Le nœud source et le nœud cible sont sur le même site.

Description de la tâche

Utilisez la procédure Move ADC pour déplacer manuellement le service ADC entre les nœuds de stockage. Par exemple, vous pouvez redistribuer les services ADC entre les nœuds ou déplacer le service ADC vers un nœud plus performant.

Cette procédure déplace les services ADC, IDNT, ACCT et RSM d'un nœud de stockage vers un autre sur le même site. Les services RSM, IDNT et ACCT dépendent du service ADC, ils se déplacent donc automatiquement lorsque le service ADC se déplace.



- Il n'est pas nécessaire de déplacer manuellement le service ADC avant "[conversion d'un nœud de stockage en nœud de données uniquement](#)" ou de mettre hors service un nœud de stockage. Ces procédures déplacent automatiquement le service ADC lorsque cela est requis. Consultez "[Qu'est-ce que le quorum ADC ?](#)" pour plus de détails sur les exigences.
- StorageGRID déplace le service ADC vers les nœuds de stockage les plus récents qui répondent aux exigences d'hébergement du service.

Étapes

1. Enregistrez les ID de nœud des nœuds source et cible.

Dans l'API de gestion de grille, l'ID du nœud source est appelé `sourceNodeId`. L'ID du nœud cible est appelé `targetNodeId`.

2. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Sélectionnez **aller à la documentation privée de l'API**.
4. Sélectionnez le POST `/private/move-adc/start` opération. Consultez "[Émettre des requêtes API](#)" pour plus d'informations.

Pendant la procédure, les deux nœuds redémarreront en séquence. Le nœud source redémarre en premier, suivi du nœud cible.

5. Vous pouvez utiliser GET `/private/move-adc` pour surveiller la procédure. Si des erreurs surviennent, sélectionnez POST `/private/move-adc/retry` pour réessayer la procédure.
6. "[Télécharger un package de récupération](#)" après avoir terminé cette procédure.

Convertir un nœud de stockage StorageGRID en un nœud de données uniquement

Pour augmenter les performances, vous pouvez convertir des nœuds de stockage non ADC plus lents en nœuds de stockage de données uniquement.

Il est logique d'utiliser un nœud de stockage exclusivement pour les données si les performances de vos nœuds de stockage diffèrent. Par exemple, pour augmenter les performances, vous pouvez disposer de nœuds de stockage sur disque rotatif haute capacité uniquement en données et accompagnés de nœuds de stockage haute performance pour métadonnées uniquement.

De plus, vous pouvez obtenir davantage de capacité de métadonnées en supprimant les nœuds à faible RAM de Cassandra, ce qui augmente la limite de capacité de métadonnées par nœud. ["Gérer le stockage des métadonnées d'objet"](#) .

Lors de la conversion de nœuds de données uniquement, la grille doit contenir au moins trois nœuds de stockage combinés ou de métadonnées uniquement par site.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Le nœud de stockage n'est pas un nœud de métadonnées uniquement ou un nœud de données uniquement.
- Si le nœud de stockage contient le service ADC, plus de deux nœuds de stockage ADC sont en ligne sur la grille, et des nœuds de stockage non-ADC sont disponibles sur le même site pour héberger le service ADC.
- Il y a suffisamment d'espace de métadonnées sur d'autres nœuds du site (ou vous avez ["élargi votre grille"](#)) pour héberger les métadonnées qui migreront à partir du nœud de stockage que vous convertissez.



- Si les métadonnées qui migrent vers d'autres nœuds sur le même site dépassent la taille du ["espace réservé aux métadonnées"](#) , la grille deviendra instable.
- Une fois la conversion lancée, vous ne pourrez plus étendre la grille.

Description de la tâche

Utilisez cette procédure pour convertir un ou plusieurs nœuds de stockage combinés en nœuds de données uniquement. Si un nœud de stockage contient le service ADC, le service est automatiquement déplacé vers un autre nœud de stockage du même site lors de la conversion.

En plus de convertir le nœud de stockage, cette procédure désaffecte Cassandra du nœud. Toutes les métadonnées seront migrées vers des nœuds de stockage combinés ou contenant uniquement des métadonnées. Selon la quantité de métadonnées à migrer, cette procédure peut prendre jusqu'à plusieurs jours par nœud.



En règle générale, vous pouvez convertir jusqu'à 10 nœuds à la fois si l'utilisation des métadonnées par nœud est inférieure à 1 To. Si l'utilisation des métadonnées par nœud est supérieure à 1 To, convertissez jusqu'à 5 nœuds par procédure à la place.



StorageGRID déplace le service ADC vers les nœuds de stockage les plus récents qui répondent aux exigences d'hébergement du service.

Étapes

1. Enregistrez les ID de nœud des nœuds de stockage non ADC que vous souhaitez convertir.
2. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Sélectionnez **aller à la documentation privée de l'API**.
4. Sélectionnez le POST `/private/convert-to-data-only-node/start` opération. Consultez ["Émettre des requêtes API"](#) pour plus d'informations.

Chaque nœud redémarrera pendant la procédure.

5. Vous pouvez utiliser `GET /private/convert-to-data-only-node` pour surveiller la procédure. Si des erreurs surviennent, sélectionnez `POST /private/convert-to-data-only-node/retry` pour réessayer la procédure.
6. ["Télécharger un package de récupération"](#) après avoir terminé cette procédure.

Procédures de redémarrage, d'arrêt et d'alimentation

Effectuez un redémarrage progressif de StorageGRID

Vous pouvez effectuer un redémarrage en continu pour redémarrer plusieurs nœuds grid sans interrompre le 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 ["Maintenance ou autorisation d'accès racine"](#).

Description de la 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 ["Règles de sécurité TLS et SSH"](#). Lorsque le mode FIPS est modifié, vous devez redémarrer tous les nœuds pour appliquer la modification.



Si vous n'avez besoin de redémarrer qu'un seul nœud, vous pouvez ["Redémarrez le nœud à partir de l'onglet tâches"](#).

Lorsque StorageGRID redémarre des nœuds de la grille, il exécute la `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 en continu peut redémarrer plusieurs nœuds en même temps, à l'exception des cas suivants :

- 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.

Ces nœuds sont redémarrés séquentiellement afin de s'assurer que les groupes haute disponibilité, 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. C'est pourquoi le nœud d'administration principal est redémarré en dernier.

Effectuer un redémarrage en continu

Sélectionnez les nœuds que vous souhaitez redémarrer, vérifiez vos sélections, démarrez la procédure de redémarrage et surveillez leur progression.

Sélectionnez les nœuds

Dans un premier temps, accédez à la page de redémarrage en roulant et sélectionnez les nœuds que vous souhaitez redémarrer.

Étapes

1. Sélectionnez **Maintenance > Tâches > Redémarrage progressif**.
2. Consultez 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 grid. 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 **Alert summary**.



Pour afficher toutes les alertes actuelles d'un nœud, vous pouvez également sélectionner le **Nœuds > onglet vue d'ensemble**.

4. Vous pouvez également effectuer les actions recommandées pour résoudre les alertes en cours.
5. Si tous les nœuds sont connectés et que vous souhaitez les redémarrer tous, cochez la case dans l'entête de la table et sélectionnez **Sélectionner tout**. Sinon, sélectionnez chaque nœud que vous souhaitez redémarrer.

Vous pouvez utiliser les options de filtre de la table pour afficher les sous-ensembles de nœuds. Par exemple, vous pouvez afficher et sélectionner uniquement les nœuds de stockage ou tous les nœuds d'un site donné.

6. Sélectionnez **sélection de revue**.

Revoir la sélection

Cette étape vous permet de déterminer le temps nécessaire à la procédure de redémarrage total et de confirmer que vous avez sélectionné les nœuds appropriés.

1. Sur la page de sélection vérifier, consultez le récapitulatif qui indique le nombre de nœuds qui seront redémarrés et la durée totale estimée pour tous les nœuds.
2. Si vous le souhaitez, pour supprimer un nœud spécifique de la liste de redémarrage, sélectionnez **Supprimer**.
3. Pour ajouter d'autres nœuds, sélectionnez **étape précédente**, sélectionnez les nœuds supplémentaires et sélectionnez **sélection de révision**.
4. Lorsque vous êtes prêt à démarrer la procédure de redémarrage en continu 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 de nouveau disponible, vous devez recharger la page de redémarrage en roulant.

Surveiller un redémarrage en continu

Pendant l'exécution de la procédure de redémarrage en continu, vous pouvez le surveiller depuis le nœud d'administration principal.

Étapes

1. Examinez la progression globale de l'opération, qui comprend les informations suivantes :
 - Nombre de nœuds redémarrés
 - Nombre de nœuds en cours de redémarrage
 - Nombre de nœuds qui restent 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 pour 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 en roulant

Vous pouvez arrêter la procédure de redémarrage en continu à partir du nœud d'administration principal. Lorsque vous arrêtez la procédure, tous les nœuds dont l'état est « Arrêt des services », « redémarrage du système » ou « démarrage des services » complètent 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. A partir de l'étape **redémarrage du moniteur**, sélectionnez **Arrêter la procédure de redémarrage**.

Redémarrer le nœud StorageGRID depuis l'onglet Tâches

Vous pouvez redémarrer un nœud de grid individuel à partir de l'onglet tâches de la page nœuds.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Si vous redémarrez le nœud d'administration principal ou tout nœud de stockage, vous avez examiné les

points suivants :

- Lorsque vous redémarrez le nœud d'administration principal, votre navigateur perd temporairement l'accès au gestionnaire de grille.
- Si vous redémarrez au moins deux nœuds de stockage sur un site donné, il se peut que vous ne puissiez pas accéder à certains objets pendant la durée du redémarrage. Ce problème peut se produire si une règle ILM utilise l'option d'acquisition **Dual Commit** (ou si une règle indique **Balanced** et qu'il n'est pas possible de créer immédiatement toutes les copies requises). Dans ce cas, StorageGRID engagera des objets récemment ingérés dans deux nœuds de stockage sur le même site et évaluera ILM plus tard.
- Pour vous assurer que vous pouvez accéder à tous les objets lors du redémarrage d'un nœud de stockage, arrêtez de les ingérer sur un site pendant environ une heure avant de redémarrer le nœud.

Description de la tâche

Lorsque StorageGRID redémarre un nœud grid, elle émet la `reboot` commande sur le 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.



Si vous devez redémarrer plusieurs nœuds, vous pouvez utiliser le ["procédure de redémarrage en roulant"](#).

Étapes

1. Sélectionnez **Nœuds**.
2. Sélectionnez le nœud de grille que vous souhaitez redémarrer.
3. Sélectionnez l'onglet **tâches**.
4. Sélectionnez **Reboot**.

Une boîte de dialogue de confirmation s'affiche. Si vous redémarrez le nœud d'administration principal, la boîte de dialogue de confirmation vous rappelle que la connexion de votre navigateur au Grid Manager sera interrompue temporairement lorsque les services sont arrêtés.

5. Entrez la phrase de passe de provisionnement et sélectionnez **OK**.
6. Attendez que le nœud redémarre.

La fermeture des services peut prendre un certain temps.

Lorsque le nœud redémarre, l'icône grise (arrêt administratif) s'affiche pour le nœud sur la page nœuds. Lorsque tous les services ont redémarré et que le nœud est correctement connecté à la grille, la page nœuds doit afficher l'état normal (aucune icône à gauche du nom du nœud), ce qui indique qu'aucune alerte n'est active et que le nœud est connecté à la grille.

Redémarrer le nœud StorageGRID depuis l'invite de commandes

Si vous devez surveiller de plus près l'opération de redémarrage ou si vous ne parvenez pas à accéder au Gestionnaire de grille, vous pouvez vous connecter au nœud de grille et exécuter la commande de redémarrage de Server Manager à partir du shell de

commande.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Si vous le souhaitez, arrêtez les services : `service servermanager stop`

L'arrêt des services est une étape facultative mais recommandée. Les services peuvent prendre jusqu'à 15 minutes pour s'arrêter, et vous pouvez vous connecter au système à distance pour surveiller le processus d'arrêt avant de redémarrer le nœud à l'étape suivante.

3. Redémarrer le nœud grid : `reboot`
4. Déconnectez-vous du shell de commande : `exit`

Arrêter le nœud StorageGRID

Vous pouvez arrêter un nœud de grille à partir du shell de commande du nœud.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Description de la tâche

Avant d'effectuer cette procédure, consultez les considérations suivantes :

- En général, vous ne devez pas arrêter plusieurs nœuds à la fois pour éviter les perturbations.
- N'arrêtez pas un nœud pendant une procédure de maintenance sauf instruction explicite de la documentation ou du support technique.
- Le processus d'arrêt dépend de l'endroit où le nœud est installé, comme suit :
 - L'arrêt d'un nœud VMware arrête la machine virtuelle.
 - L'arrêt d'un nœud Linux arrête le conteneur.
 - L'arrêt d'un nœud d'appliance StorageGRID arrête le contrôleur de calcul.
- Si vous prévoyez d'arrêter plusieurs nœuds de stockage d'un site, arrêtez d'ingérer les objets sur ce site pendant environ une heure avant d'arrêter les nœuds.

Si une règle ILM utilise l'option d'ingestion **Dual Commit** (ou si une règle utilise l'option **Balanced** et que toutes les copies requises ne peuvent pas être créées immédiatement), StorageGRID valide immédiatement tous les objets nouvellement ingérés sur deux nœuds de stockage sur le même site et évalue ILM ultérieurement. Si plusieurs nœuds de stockage d'un site sont arrêtés, il se peut que vous ne

puissiez pas accéder aux objets récemment acquis pendant la durée de l'arrêt. Les opérations d'écriture peuvent également échouer si un nombre trop faible de nœuds de stockage restent disponibles sur le site. Voir "[Gestion des objets avec ILM](#)".

Étapes

1. Connectez-vous au nœud grid :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêter tous les services : `service servermanager stop`

L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.

3. Si le nœud s'exécute sur une machine virtuelle VMware ou s'il s'agit d'un nœud d'appliance, exécutez la commande `shutdown` : `shutdown -h now`

Exécutez cette étape quel que soit le résultat de la `service servermanager stop` commande.



Après avoir exécutée la `shutdown -h now` commande sur un nœud d'appliance, vous devez mettre l'appliance hors/sous tension pour redémarrer le nœud.

Pour l'appliance, cette commande arrête le contrôleur, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.

4. Si vous mettez un nœud d'appliance hors tension, suivez les étapes indiquées pour l'appliance.

SG6160

- a. Mettez le contrôleur de stockage SG6100-CN hors tension.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Dans la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Vérifiez que toutes les opérations ont été effectuées avant de passer à l'étape suivante.
- d. Mettez les deux boutons marche/arrêt sur le tiroir contrôleur et attendez que toutes les LED du tiroir contrôleur s'éteignent.

SG5700

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.

SG100 ou SG1000

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

Mettre hors tension un hôte StorageGRID

Avant de mettre un hôte hors tension, vous devez arrêter les services de tous les nœuds du grid sur cet hôte.

Étapes

1. Connectez-vous au nœud grid :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Arrêter tous les services en cours d'exécution sur le nœud : `service servermanager stop`

L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.

3. Répétez les étapes 1 et 2 pour chaque nœud de l'hôte.
4. Si vous disposez d'un hôte Linux :
 - a. Connectez-vous au système d'exploitation hôte.
 - b. Arrêter le nœud : `storagegrid node stop`
 - c. Arrêtez le système d'exploitation hôte.
5. Si le nœud s'exécute sur une machine virtuelle VMware ou s'il s'agit d'un nœud d'appliance, exécutez la commande `shutdown : shutdown -h now`

Exécutez cette étape quel que soit le résultat de la `service servermanager stop` commande.



Après avoir exécutée la `shutdown -h now` commande sur un nœud d'appliance, vous devez mettre l'appliance hors/sous tension pour redémarrer le nœud.

Pour l'appliance, cette commande arrête le contrôleur, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.

6. Si vous mettez un nœud d'appliance hors tension, suivez les étapes indiquées pour l'appliance.

SG6160

- a. Mettez le contrôleur de stockage SG6100-CN hors tension.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Dans la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Vérifiez que toutes les opérations ont été effectuées avant de passer à l'étape suivante.
- d. Mettez les deux boutons marche/arrêt sur le tiroir contrôleur et attendez que toutes les LED du tiroir contrôleur s'éteignent.

SG5700

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.

SG110 ou SG1100

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG100 ou SG1000

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

7. Déconnectez-vous du shell de commande : `exit`

Informations associées

- ["Appliances de stockage SGF6112 et SG6160"](#)
- ["Systèmes de stockage SG6000"](#)
- ["Systèmes de stockage SG5700"](#)
- ["Systèmes de stockage SG5800"](#)
- ["Appliances de services SG110 et SG1100"](#)
- ["Appliances de services SG100 et SG1000"](#)

Mettez hors tension puis sous tension tous les nœuds StorageGRID

Vous devrez peut-être arrêter l'intégralité de votre système StorageGRID, par exemple si vous déplacez un data Center. Ces étapes fournissent une vue d'ensemble de haut niveau de la séquence recommandée pour effectuer un arrêt et un démarrage contrôlés.

Lorsque vous mettez hors tension tous les nœuds d'un site ou d'une grille, vous ne pouvez pas accéder aux objets ingérés tant que les nœuds de stockage sont hors ligne.

Arrêtez les services et arrêtez les nœuds de la grille

Avant de mettre un système StorageGRID hors tension, vous devez arrêter tous les services exécutés sur chaque nœud de grid, puis arrêter toutes les machines virtuelles VMware, les moteurs de conteneurs et les appliances StorageGRID.

Description de la tâche

Arrêtez d'abord les services sur les nœuds d'administration et les nœuds de passerelle, puis arrêtez les services sur les nœuds de stockage.

Cette approche vous permet d'utiliser le nœud d'administration principal pour surveiller l'état des autres nœuds de la grille aussi longtemps que possible.



Si un seul hôte comprend plusieurs nœuds de grille, n'arrêtez pas l'hôte tant que vous n'avez pas arrêté tous les nœuds de cet hôte. Si l'hôte inclut le nœud d'administration principal, arrêtez l'hôte en dernier.



Si nécessaire, vous pouvez ["Migrer des nœuds d'un hôte Linux vers un autre"](#) effectuer la maintenance de l'hôte sans affecter les fonctionnalités ou la disponibilité de votre grille.

Étapes

1. L'accès SSH externe est bloqué par défaut. Si nécessaire, ["autoriser temporairement l'accès"](#).
2. Arrêtez toutes les applications client d'accéder à la grille.
3. Connectez-vous à chaque nœud de passerelle :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

4. Arrêter tous les services en cours d'exécution sur le nœud : `service servermanager stop`

L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.

5. 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 exécutez la `service servermanager stop` commande pour arrêter les services sur un nœud de stockage de l'appliance, vous devez mettre l'appliance hors/sous tension pour redémarrer le nœud.

6. Pour le nœud d'administration principal, répétez les étapes pour [connectez-vous au nœud](#) et [arrêt de tous les services du nœud](#).
7. Pour les nœuds qui s'exécutent sur des hôtes Linux :
 - a. Connectez-vous au système d'exploitation hôte.
 - b. Arrêter le nœud : `storagegrid node stop`
 - c. Arrêtez le système d'exploitation hôte.
8. Pour les nœuds qui s'exécutent sur des machines virtuelles VMware et pour les nœuds de stockage de l'appliance, exécutez la commande `shutdown : shutdown -h now`

Exécutez cette étape quel que soit le résultat de la `service servermanager stop` commande.

Pour l'appliance, cette commande arrête le contrôleur de calcul, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.

9. Si vous disposez de nœuds d'appliance, suivez les étapes correspondant à votre appliance.

SG110 ou SG1100

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG100 ou SG1000

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6160

- a. Mettez le contrôleur de stockage SG6100-CN hors tension.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Mettez l'appareil hors tension.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Dans la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Vérifiez que toutes les opérations ont été effectuées avant de passer à l'étape suivante.
- d. Mettez les deux boutons marche/arrêt sur le tiroir contrôleur et attendez que toutes les LED du tiroir contrôleur s'éteignent.

SG5700

- a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

- b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.

10. Si nécessaire, déconnectez-vous du shell de commande : `exit`

La grille StorageGRID est maintenant arrêtée.

11. Si vous avez autorisé l'accès SSH externe, "[bloquer l'accès](#)" lorsque vous avez terminé d'arrêter les nœuds.

Démarrer les nœuds grid

Si possible, mettez les nœuds grid sous tension dans l'ordre suivant :

- Mettez d'abord les nœuds d'administration sous tension.
- Appliquer l'alimentation aux nœuds de passerelle en dernier.



Si un hôte comprend plusieurs nœuds de grid, ces nœuds se remettent automatiquement en ligne lorsque vous mettez l'hôte sous tension.

Étapes

1. Mettez les hôtes sous tension pour le nœud d'administration principal et tous les nœuds d'administration non primaires.



Vous ne pouvez pas vous connecter aux nœuds d'administration tant que les nœuds de stockage n'ont pas été redémarrés.

2. Mettez les hôtes sous tension pour tous les nœuds de stockage.

Vous pouvez mettre ces nœuds sous tension dans n'importe quel ordre.

3. Mettez les hôtes sous tension pour tous les nœuds de passerelle.
4. Connectez-vous au Grid Manager.
5. Sélectionnez **Nœuds** 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 associées

- "[Appliances de stockage SGF6112 et SG6160](#)"
- "[Appliances de services SG110 et SG1100](#)"
- "[Appliances de services SG100 et SG1000](#)"
- "[Systèmes de stockage SG6000](#)"
- "[Systèmes de stockage SG5800](#)"
- "[Systèmes de stockage SG5700](#)"

Procédures de remap de port

Supprimer les remappages de ports sur les appliances StorageGRID

Si vous souhaitez configurer un nœud final pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré en tant que port mappé sur d'un remappage de port, vous devez d'abord supprimer le plan de port existant, sinon le nœud final ne sera pas effectif. Vous devez exécuter un script sur chaque nœud d'administration et nœud de passerelle qui comporte des ports en conflit avec des mappages afin de supprimer tous les mappages de ports du nœud.

Description de la tâche

Cette procédure supprime tous les mappages de ports. Si vous devez conserver certains des plans, contactez le support technique.

Pour plus d'informations sur la configuration des noeuds finaux de l'équilibreur de charge, voir ["Configuration des terminaux d'équilibrage de charge"](#).



Si le remap de port fournit un accès client, reconfigurez le client pour qu'il utilise un autre port comme point final d'équilibrage de charge afin d'éviter toute perte de service. Dans le cas contraire, la suppression du mappage de port entraîne une perte de l'accès client et doit être planifiée de manière appropriée.



Cette procédure ne fonctionne pas pour un système StorageGRID déployé en tant que conteneur sur les hôtes bare Metal. Voir les instructions pour ["suppression de mappages de port sur les hôtes bare metal"](#).

Étapes

1. L'accès SSH externe est bloqué par défaut. Si nécessaire, ["autoriser temporairement l'accès"](#) .
2. 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 mise en conteneurs exécutant StorageGRID.

- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Exécutez le script suivant : `remove-port-remap.sh`
4. Redémarrez le nœud : `reboot`
5. Déconnectez-vous du shell de commande : `exit`
6. Répétez ces étapes sur chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés.
7. Si vous avez autorisé l'accès SSH externe, ["bloquer l'accès"](#) lorsque vous avez terminé de supprimer les remappages de ports.

Informations associées

- ["Ports utilisés pour les communications externes"](#)

Supprimer les réaffectations de ports StorageGRID sur les hôtes physiques

Si vous souhaitez configurer un noeud final pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré en tant que port mappé sur d'un remappage de port, vous devez d'abord supprimer le plan de plan de port existant, sinon le noeud final ne sera pas effectif.

Description de la tâche

Si vous exécutez StorageGRID sur des hôtes bare Metal, suivez cette procédure à la place de la procédure générale de suppression des mappages de ports. Vous devez modifier le fichier de configuration de nœud pour chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés pour supprimer tous les mappages de port du nœud et redémarrer le nœud.



Cette procédure supprime tous les mappages de ports. Si vous devez conserver certains des plans, contactez le support technique.

Pour plus d'informations sur la configuration des terminaux de l'équilibreur de charge, reportez-vous aux instructions d'administration de StorageGRID.



Cette procédure peut entraîner une perte temporaire de service au redémarrage des nœuds.

Étapes

1. Connectez-vous à l'hôte supportant le nœud. Connectez-vous en tant que root ou avec un compte disposant de l'autorisation sudo.
2. Exécutez la commande suivante pour désactiver temporairement le nœud : `sudo storagegrid node stop node-name`
3. À l'aide d'un éditeur de texte tel que vim ou pico, modifiez le fichier de configuration de nœud pour le nœud.

Le fichier de configuration de nœud se trouve à l'adresse `/etc/storagegrid/nodes/node-name.conf`.

4. Recherchez la section du fichier de configuration du nœud qui contient les mappages de port.

Voir les deux dernières lignes dans l'exemple suivant.

```

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = DedicatedInterface
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 = DedicatedInterface
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 = DedicatedInterface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443

```

5. Modifiez LES entrées `PORT_REMAP` et `PORT_REMAPPAGE_INBOUND` pour supprimer les remapes de port.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Exécutez la commande suivante pour valider les modifications apportées au fichier de configuration du nœud : `sudo storagegrid node validate node-name`

Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

7. Exécutez la commande suivante pour redémarrer le nœud sans remmaps de port : `sudo storagegrid node start node-name`
8. Connectez-vous au nœud en tant qu'administrateur à l'aide du mot de passe indiqué dans le `Passwords.txt` fichier.
9. Vérifiez que les services démarrent correctement.
 - a. Afficher la liste des États de tous les services sur le serveur : `sudo storagegrid-status`

L'état est mis à jour automatiquement.

b. Attendez que tous les services aient l'état en cours d'exécution ou vérifié.

c. Quitter l'écran d'état :Ctrl+C

10. Répétez ces étapes sur chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés.

Procédures de Server Manager

Afficher l'état et la version de StorageGRID Server Manager

Pour chaque nœud de grille, vous pouvez afficher l'état et la version actuels de Server Manager exécuté sur ce nœud de grille. Vous pouvez également obtenir l'état actuel de tous les services exécutés sur ce nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

a. Entrez la commande suivante : `ssh admin@grid_node_IP`

b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Afficher l'état actuel de Server Manager exécuté sur le nœud de grille : **`service servermanager status`**

L'état actuel de Server Manager s'exécutant sur le nœud de la grille est signalé (en cours d'exécution ou non). Si l'état de Server Manager est `running`, l'heure à laquelle il a été exécuté depuis le dernier démarrage est indiquée. Par exemple :

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Afficher la version actuelle de Server Manager s'exécutant sur un nœud de grille : **`service servermanager version`**

La version actuelle est répertoriée. Par exemple :

```
11.1.0-20180425.1905.39c9493
```

4. Déconnectez-vous du shell de commande : **`exit`**

Afficher l'état actuel de tous les services StorageGRID

Vous pouvez afficher à tout moment l'état actuel de tous les services s'exécutant sur un nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

- Entrez la commande suivante : `ssh admin@grid_node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Par exemple, la sortie du nœud d'administration principal indique l'état actuel des services AMS, CMN et NMS en cours d'exécution. Cette sortie est immédiatement mise à jour si l'état d'un service change.

```
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
attrDownSamp1       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 s'exécutant sur le nœud de grille : `/usr/local/servermanager/reader.rb`

Ce rapport contient les mêmes informations que le rapport mis à jour en continu, mais il n'est pas mis à

jour si l'état d'un service change.

5. Déconnectez-vous du shell de commande : `exit`

Démarrez StorageGRID Server Manager et tous les services

Vous devrez peut-être démarrer Server Manager, qui démarre également tous les services sur le nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Le démarrage de Server Manager sur un nœud de la grille sur lequel il est déjà en cours d'exécution entraîne le redémarrage de Server Manager et de tous les services sur le nœud de la grille.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Démarrez Server Manager : `service servermanager start`
3. Déconnectez-vous du shell de commande : `exit`

Redémarrez StorageGRID Server Manager et tous les services

Vous devrez peut-être redémarrer Server Manager et tous les services en cours d'exécution sur un nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Redémarrez Server Manager et tous les services sur le nœud de grille : `service servermanager`

`restart`

Server Manager et tous les services du nœud de la grille sont arrêtés, puis redémarrés.



L'utilisation de la commande est la même que l'utilisation de `restart` la `stop` commande suivie de celle-ci `start`.

3. Déconnectez-vous du shell de commande : `exit`

Arrêtez StorageGRID Server Manager et tous les services

Server Manager est conçu pour fonctionner en permanence, mais il peut être nécessaire d'arrêter Server Manager et tous les services exécutés sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Arrêtez Server Manager et tous les services s'exécutant sur le nœud de grille : `service servermanager stop`

Server Manager et tous les services exécutés sur le nœud de la grille sont normalement terminés. L'arrêt des services peut prendre jusqu'à 15 minutes.

3. Déconnectez-vous du shell de commande : `exit`

Afficher l'état actuel d'un service StorageGRID

Vous pouvez consulter à tout moment l'état actuel d'un service en cours d'exécution sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Afficher l'état actuel d'un service exécuté sur un nœud de grille : ``service serviceename status`` l'état actuel du service demandé s'exécutant sur le nœud de grille est signalé (en cours d'exécution ou non). Par exemple :

```
cmn running for 1d, 14h, 21m, 2s
```

3. Déconnectez-vous du shell de commande : `exit`

Arrêter un service StorageGRID

Certaines procédures de maintenance exigent d'arrêter un seul service tout en maintenant d'autres services sur le nœud de la grille en cours d'exécution. N'arrêtez les services individuels que si vous y êtes invité par une procédure de maintenance.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Lorsque vous utilisez ces étapes pour « arrêter administrativement » un service, Server Manager ne redémarre pas automatiquement le service. Vous devez démarrer le service unique manuellement ou redémarrer Server Manager.

Si vous devez arrêter le service LDR sur un nœud de stockage, veillez à savoir qu'il peut prendre un certain temps pour arrêter le service s'il existe des connexions actives.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Arrêter un service individuel : `service servicename stop`

Par exemple :

```
service ldr stop
```



L'arrêt des services peut prendre jusqu'à 11 minutes.

3. Déconnectez-vous du shell de commande : `exit`

Informations associées

["Forcer la fin du service"](#)

Forcer un service StorageGRID à se terminer

Si vous devez arrêter immédiatement un service, vous pouvez utiliser `force-stop` la commande.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Forcer manuellement la fin du service : `service servicename force-stop`

Par exemple :

```
service ldr force-stop
```

Le système attend 30 secondes avant de mettre fin au service.

3. Déconnectez-vous du shell de commande : `exit`

Démarrer ou redémarrer un service StorageGRID

Vous devrez peut-être démarrer un service qui a été arrêté, ou vous devrez peut-être arrêter et redémarrer un service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Choisissez la commande à exécuter, en fonction du type de service en cours d'exécution ou arrêté.

- Si le service est actuellement arrêté, utiliser `start` la commande pour démarrer le service manuellement : `service servicename start`

Par exemple :

```
service ldr start
```

- Si le service est en cours d'exécution, utilisez la `restart` commande pour arrêter le service, puis redémarrez-le : `service servicename restart`

Par exemple :

```
service ldr restart
```

+



L'utilisation de la commande est la même que l'utilisation de `restart` la `stop` commande suivie de celle-ci `start`. Vous pouvez émettre un problème `restart` même si le service est actuellement arrêté.

3. Déconnectez-vous du shell de commande : `exit`

Utilisez un fichier DoNotStart StorageGRID

Si vous effectuez diverses procédures de maintenance ou de configuration sous la direction du support technique, il se peut que vous soyez invité à utiliser un fichier DoNotStart pour empêcher les services de démarrer lorsque Server Manager est démarré ou redémarré.



Vous ne devez ajouter ou supprimer un fichier DoNotStart que si le support technique vous a demandé de le faire.

Pour empêcher le démarrage d'un service, placez un fichier DoNotStart dans le répertoire du service que vous souhaitez empêcher de démarrer. Au démarrage, Server Manager recherche le fichier DoNotStart. Si le fichier est présent, le service (et les services qui en dépendent) ne peut pas démarrer. Lorsque le fichier DoNotStart est supprimé, le service précédemment arrêté démarre au prochain démarrage ou redémarrage de Server Manager. Les services ne sont pas automatiquement démarrés lorsque le fichier DoNotStart est supprimé.

Le moyen le plus efficace d'empêcher le redémarrage de tous les services est d'empêcher le démarrage du service NTP. Tous les services dépendent du service NTP et ne peuvent pas s'exécuter si le service NTP n'est pas en cours d'exécution.

Ajouter le fichier DoNotStart pour le service

Vous pouvez empêcher le démarrage d'un service individuel en ajoutant un fichier DoNotStart au répertoire de ce service sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Ajouter un fichier DoNotStart : `touch /etc/sv/service/DoNotStart`

où `service` est le nom du service à empêcher de démarrer. Par exemple :

```
touch /etc/sv/ldr/DoNotStart
```

Un fichier DoNotStart est créé. Aucun contenu de fichier n'est nécessaire.

Lorsque Server Manager ou le nœud de la grille est redémarré, Server Manager redémarre, mais le service ne le fait pas.

3. Déconnectez-vous du shell de commande : `exit`

Supprimez le fichier DoNotStart pour le service

Lorsque vous supprimez un fichier DoNotStart qui empêche le démarrage d'un service, vous devez démarrer ce service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Supprimez le fichier DoNotStart du répertoire de service : `rm /etc/sv/service/DoNotStart`

où `service` est le nom du service. Par exemple :

```
rm /etc/sv/ldr/DoNotStart
```

3. Démarrez le service : `service servicename start`
4. Déconnectez-vous du shell de commande : `exit`

Dépanner Server Manager dans StorageGRID

Si un problème survient lors de l'utilisation de Server Manager, vérifiez son fichier journal.

Les messages d'erreur relatifs à Server Manager sont capturés dans le fichier journal de Server Manager, qui se trouve à l'adresse suivante : `/var/local/log/servermanager.log`

Consultez ce fichier pour voir s'il contient des messages d'erreur relatifs aux échecs. Transmettez le problème au support technique si nécessaire. Il se peut que vous soyez invité à transférer les fichiers journaux au support technique.

Service avec un état d'erreur

Si vous détectez qu'un service a entré un état d'erreur, essayez de redémarrer le service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Server Manager surveille les services et redémarre tout qui s'est arrêté de façon inattendue. En cas d'échec d'un service, Server Manager tente de le redémarrer. Si trois tentatives de démarrage d'un service ont échoué dans les cinq minutes, le service passe en état d'erreur. Server Manager ne tente pas un redémarrage supplémentaire.

Étapes

1. Connectez-vous au nœud grid :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Confirmez l'état d'erreur du service : `service servicename status`

Par exemple :

```
service ldr status
```

Si le service est en état d'erreur, le message suivant est renvoyé : `servicename in error state`. Par exemple :

```
ldr in error state
```



Si l'état du service est `disabled`, reportez-vous aux instructions pour ["Suppression d'un fichier DoNotStart pour un service"](#).

3. Essayez de supprimer l'état d'erreur en redémarrant le service : `service servicename restart`

Si le service ne parvient pas à redémarrer, contactez le support technique.

4. Déconnectez-vous du shell de commande : `exit`

Procédures réseau

Mise à jour des sous-réseaux pour StorageGRID Grid Network

StorageGRID conserve une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de la grille sur le réseau Grid (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site du système StorageGRID, ainsi que tous les sous-réseaux utilisés pour les serveurs NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle réseau Grid. Lorsque vous ajoutez des nœuds de grille ou un nouveau site dans une extension, vous devrez peut-être mettre à jour ou ajouter des sous-réseaux au réseau Grid.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Les adresses réseau des sous-réseaux que vous souhaitez configurer sont définies, en notation CIDR.

Description de la tâche

Si vous effectuez une activité d'extension incluant l'ajout d'un nouveau sous-réseau, vous devez ajouter un nouveau sous-réseau à la liste de sous-réseaux réseau de la grille avant de démarrer la procédure d'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et relancer l'extension.

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
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 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

Ajoutez 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 le mot de passe 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 automatiquement configurés pour votre système StorageGRID.

Modifier un sous-réseau

Étapes

1. Sélectionnez **Maintenance > Réseau > Réseau de grille**.
2. Sélectionnez le sous-réseau à modifier et apportez les modifications nécessaires.
3. Saisissez le mot de passe de provisionnement et sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** dans la boîte de dialogue de confirmation.
5. Attendez que les modifications soient appliquées, puis téléchargez un nouveau package de récupération.
 - a. Sélectionnez **Maintenance > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.

Supprimez un sous-réseau

Étapes

1. Sélectionnez **Maintenance > Réseau > Réseau de grille**.
2. Sélectionnez l'icône de suppression  à côté du sous-réseau.
3. Entrez la phrase de passe de provisionnement et sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** dans la boîte de dialogue de confirmation.
5. Attendez que les modifications soient appliquées, puis téléchargez un nouveau package de récupération.
 - a. Sélectionnez **Maintenance > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.

Configurez les adresses IP

StorageGRID Règles d'adressage IP

Vous pouvez configurer le réseau en configurant des adresses IP pour les noeuds de la grille à l'aide de l'outil Modifier les adresses IP.

Vous devez utiliser l'outil Modifier l'IP pour apporter la plupart des modifications à la configuration réseau qui ont été initialement définies lors du déploiement de la grille. Les modifications manuelles effectuées à l'aide de commandes et de fichiers de mise en réseau Linux standard peuvent ne pas se propager à tous les services StorageGRID et ne pas persister entre les mises à niveau, redémarrages ou les procédures de restauration des nœuds.



La procédure de modification IP peut être une procédure perturbateur. Des parties de la grille peuvent être indisponibles jusqu'à l'application de la nouvelle configuration.



Si vous apportez uniquement des modifications à la liste de sous-réseaux du réseau Grid, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Dans le cas contraire, utilisez l'outil Modifier IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration du réseau ou si vous effectuez une modification du routage du réseau Grid et d'autres modifications du réseau simultanément.



Si vous souhaitez modifier l'adresse IP du réseau de la grille pour tous les nœuds de la grille, utilisez la ["procédure spéciale pour les changements à l'échelle de la grille"](#).

Interfaces Ethernet

L'adresse IP attribuée à eth0 est toujours l'adresse IP réseau du nœud de la grille. L'adresse IP attribuée à eth1 est toujours l'adresse IP du réseau Admin du nœud de la grille. L'adresse IP attribuée à eth2 est toujours l'adresse IP du réseau client du nœud de la grille.

Notez que, sur certaines plateformes, comme les appliances StorageGRID, eth0, eth1 et eth2 peuvent être des interfaces agrégées composées de ponts subordonnés ou de liaisons d'interfaces physiques ou VLAN. Sur ces plates-formes, l'onglet **SSM > Resources** peut afficher l'adresse IP de la grille, de l'administrateur et du réseau client attribuée à d'autres interfaces en plus de eth0, eth1 ou eth2.

DHCP

Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration. Vous devez utiliser les procédures de modification d'adresse IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un nœud de grille. L'utilisation de l'outil Modifier les adresses IP va rendre les adresses DHCP statiques.

Groupes haute disponibilité (HA)

- Si une interface client Network se trouve dans un groupe haute disponibilité, vous ne pouvez pas modifier l'adresse IP client Network de cette interface en une adresse qui se trouve en dehors du sous-réseau configuré pour le groupe haute disponibilité.
- Vous ne pouvez pas modifier l'adresse IP du réseau client en fonction de la valeur d'une adresse IP virtuelle existante attribuée à un groupe haute disponibilité configuré sur l'interface réseau client.
- Si une interface réseau Grid est contenue dans un groupe haute disponibilité, vous ne pouvez pas modifier l'adresse IP réseau Grid de cette interface pour la remplacer par une adresse située en dehors du sous-réseau configuré pour le groupe haute disponibilité.
- Vous ne pouvez pas modifier l'adresse IP du réseau Grid sur la valeur d'une adresse IP virtuelle existante attribuée à un groupe HA configuré sur l'interface réseau Grid.

Modifier la configuration réseau du nœud dans StorageGRID

Vous pouvez modifier la configuration réseau d'un ou plusieurs nœuds à l'aide de l'outil Modifier l'adresse IP. Vous pouvez modifier la configuration du réseau Grid, ou ajouter, modifier ou supprimer les réseaux Admin ou Client. Vous pouvez également modifier les paramètres IP LAN d'un nœud BMC.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la 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. Voir le StorageGRID ["instructions d'installation"](#) pour votre système d'exploitation Linux.

Appareils : sur les appareils StorageGRID, si le réseau client ou administrateur n'a pas été configuré dans le programme d'installation de l'appliance StorageGRID pendant l'installation initiale, le réseau ne peut pas être ajouté en utilisant uniquement l'outil Modifier IP. Tout d'abord, vous devez ["mettre l'appareil en mode de maintenance"](#) configurer les liaisons, remettre l'appliance en mode de fonctionnement normal, puis utiliser l'outil Modifier IP pour modifier la configuration réseau. Voir la ["procédure de configuration des liens réseau"](#).

Vous pouvez modifier l'adresse IP, le masque de sous-réseau, la passerelle ou la valeur MTU d'un ou plusieurs nœuds sur n'importe quel réseau.

Vous pouvez également ajouter ou supprimer un nœud d'un réseau client ou d'un réseau d'administration :

- Vous pouvez ajouter un nœud à un réseau client ou à un réseau d'administration en ajoutant une adresse IP/un masque de sous-réseau sur ce réseau au nœud.
- Vous pouvez supprimer un nœud d'un réseau client ou d'un réseau d'administration en supprimant l'adresse IP/le masque de sous-réseau du nœud sur ce réseau.

Impossible de supprimer des nœuds du réseau Grid.



Les échanges d'adresses IP ne sont pas autorisés. Si vous devez échanger des adresses IP entre des 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 la modification de l'adresse IP, vous devez mettre à jour ou reconfigurer l'approbation de partie de confiance du nœud dans Active Directory Federation Services (AD FS) avec la nouvelle adresse IP. Consultez les instructions de configuration de l'authentification unique (SSO) à l'aide de ["OIDC"](#) ou ["SAML"](#).



Toutes les modifications que vous apportez au réseau à l'aide de l'outil Modifier IP sont propagées au micrologiciel du programme d'installation des appliances StorageGRID. Ainsi, si le logiciel StorageGRID est réinstallé sur une appliance ou si une appliance est placée en mode de maintenance, la configuration réseau est correcte.

Étapes

1. L'accès SSH externe est bloqué par défaut. Si nécessaire, ["autoriser temporairement l'accès"](#).
2. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Démarrez l'outil Modifier IP en entrant la commande suivante : `change-ip`
4. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche.


```

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. Vous pouvez également sélectionner **1** pour choisir les nœuds à mettre à jour. Sélectionnez ensuite l'une des options suivantes :

- **1** : nœud unique — sélectionnez par nom
- **2** : nœud unique — sélectionnez par site, puis par nom
- **3** : nœud unique — sélectionnez par adresse IP actuelle
- **4** : Tous les nœuds d'un site
- **5** : tous les nœuds de la grille

Remarque : si vous souhaitez mettre à jour tous les nœuds, laissez "tous" rester sélectionnés.

Une fois votre sélection effectuée, le menu principal s'affiche, le champ **nœuds sélectionnés** étant mis à jour pour refléter votre choix. Toutes les actions suivantes sont uniquement réalisées sur les nœuds affichés.

6. 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, administrateur ou client), le type de données (IP/masque, passerelle, ou MTU), et valeur actuelle.

La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou de la MTU d'une interface configurée par DHCP changera l'interface en mode statique. Lorsque vous sélectionnez pour modifier une interface configurée par DHCP, un avertissement s'affiche pour vous informer que l'interface passe en mode statique.

Les interfaces configurées comme `fixed` ne peuvent pas être modifiées.

- b. Pour définir une nouvelle valeur, saisissez-la dans le format indiqué pour la valeur actuelle.
- c. Pour laisser la valeur actuelle inchangée, appuyez sur **entrée**.

- d. Si le type de données est `IP/mask`, vous pouvez supprimer le réseau Admin ou client du nœud en entrant **d** ou **0.0.0.0/0**.
- e. Après avoir modifié tous les noeuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.

7. Vérifiez vos modifications en sélectionnant l'une des options suivantes :

- **5** : affiche les modifications dans la sortie isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en évidence en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie :

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- **6** : affiche les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré. L'affichage correct dépend de votre client terminal prenant en charge les séquences d'échappement VT100 nécessaires.

8. Sélectionnez l'option **7** pour valider toutes les modifications.

Cette validation garantit que les règles pour les réseaux Grid, Admin et client, telles que l'absence de sous-réseaux superposés, ne sont pas violées.

Dans cet exemple, la validation a renvoyé des erreurs.

```

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

```

9. Une fois la validation terminée, choisissez l'une des options suivantes :

- **8**: Enregistrer les modifications non appliquées.

Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les modifications non appliquées.

- **10** : appliquer la nouvelle configuration réseau.

10. Si vous avez sélectionné l'option **10**, choisissez l'une des options suivantes :

- **Appliquer** : appliquez les modifications immédiatement et redémarrez automatiquement chaque nœud si nécessaire.

Si la nouvelle configuration réseau ne nécessite aucune modification de réseau physique, vous pouvez sélectionner **appliquer** pour appliquer les modifications immédiatement. Les nœuds seront redémarrés automatiquement, si nécessaire. Les nœuds qui doivent être redémarrés s'affichent.

- **Etape** : appliquez les modifications lors du prochain redémarrage manuel des nœuds.

Si vous devez apporter des modifications de configuration de réseau physique ou virtuel pour que la nouvelle configuration de réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds affectés, effectuer les modifications de réseau physiques nécessaires et redémarrer les nœuds affectés. Si vous sélectionnez **appliquer** sans effectuer au préalable ces modifications de mise en réseau, les modifications échoueront généralement.



Si vous utilisez l'option **stage**, vous devez redémarrer le nœud le plus rapidement possible après le staging pour minimiser les interruptions.

- **Annuler**: Ne faites pas de modifications de réseau pour le moment.

Si vous n'étiez pas conscient que les modifications proposées nécessitent de redémarrer les nœuds, vous pouvez reporter les modifications pour minimiser l'impact sur les utilisateurs. Si vous sélectionnez **annuler**, vous revenez au menu principal et les modifications sont préservées pour pouvoir les appliquer ultérieurement.

Lorsque vous sélectionnez **appliquer** ou **stage**, un nouveau fichier de configuration réseau est généré, le provisionnement est effectué et les nœuds sont mis à jour avec de nouvelles informations de travail.

Pendant l'approvisionnement, la sortie affiche l'état au fur et à mesure de l'application des mises à jour.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

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.

11. Si vous avez sélectionné **stage**, suivez ces étapes une fois le provisionnement terminé :

a. Apportez les modifications nécessaires au réseau physique ou virtuel.

Modifications de mise en réseau physique : apportez les modifications nécessaires à la mise en réseau physique, en arrêtant le nœud en toute sécurité si nécessaire.

Linux : si vous ajoutez le nœud à un réseau Admin ou client pour la première fois, assurez-vous d'avoir ajouté l'interface comme décrit dans ["Linux : ajoutez des interfaces au nœud existant"](#).

a. Redémarrez les nœuds concernés.

12. Sélectionnez **0** pour quitter l'outil Modifier l'IP une fois les modifications effectuées.

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 pour le provisionnement.

14. Si vous avez autorisé l'accès SSH externe, ["bloquer l'accès"](#) lorsque vous avez terminé de modifier la configuration du réseau de nœuds.

Modification temporaire du taux de PDU LACP

Pour effectuer des opérations de maintenance sur les composants réseau installés sur votre appareil, comme la mise à niveau du micrologiciel de la carte réseau, vous pouvez vérifier que le paramètre de débit PDU LACP actuel répond aux exigences de synchronisation de communication de la carte réseau. Vous pouvez basculer de manière non persistante le débit PDU LACP entre rapide (attente de 1 seconde) et lent (attente de 30 secondes), si nécessaire.



Pour apporter des modifications permanentes au taux PDU LACP, voir ["Configurer les liaisons réseau"](#).

Avant de commencer

- Le nœud d'administration est installé et en cours d'exécution.
- Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud d'administration principal :

a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`

- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Pour vérifier le paramètre de débit PDU LACP actuel, entrez la commande suivante :

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
```

3. Pour modifier temporairement le débit PDU LACP, entrez la commande suivante :

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
```

où *<speed>* est *fast* ou *slow*.

Le débit PDU LACP reviendra à son paramètre précédent lors du prochain redémarrage de l'appareil.

Modifier les paramètres IP LAN du BMC du nœud de l'appliance

Vous pouvez modifier les paramètres IP LAN d'un nœud BMC.

1. Dans Grid Manager, accédez à **Nœuds > *grid node* > Paramètres BMC**.
2. Dans la section des paramètres IP du réseau local, sélectionnez un type d'attribution d'adresse IP **Statique** ou **DHCP**.
3. Saisissez l'adresse MAC, l'adresse IPv4 (CIDR) et la passerelle par défaut du BMC.
4. Sélectionnez **Enregistrer**.

Vous pouvez également modifier ou consulter les paramètres IP LAN du BMC à l'aide de l' `PUT /bmc-configuration/root-password` ou de l' `GET /bmc-configuration/root-password` API.

Ajouter ou modifier les listes de sous-réseaux sur le réseau d'administration dans StorageGRID

Vous pouvez ajouter, supprimer ou modifier les sous-réseaux dans la liste de sous-réseaux réseau Admin d'un ou plusieurs nœuds.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux à tous les nœuds de la liste des sous-réseaux du réseau d'administration.

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
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 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. L'accès SSH externe est bloqué par défaut. Si nécessaire, "[autoriser temporairement l'accès](#)".
2. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Démarrez l'outil Modifier IP en entrant la commande suivante : `change-ip`
4. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche.

```

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. Limitez éventuellement les réseaux/nœuds sur lesquels les opérations sont effectuées. Options au choix :

- Sélectionnez les nœuds à modifier en choisissant **1**, si vous souhaitez filtrer sur des nœuds spécifiques sur lesquels effectuer l'opération. Sélectionnez l'une des options suivantes :
 - **1** : nœud unique (sélectionner par nom)
 - **2** : nœud unique (sélectionnez par site, puis par nom)
 - **3** : nœud unique (sélection par IP actuel)
 - **4** : Tous les nœuds d'un site
 - **5** : tous les nœuds de la grille
 - **0** : Retour
- Autoriser « tous » à rester sélectionné. Une fois la sélection effectuée, l'écran du menu principal s'affiche. Le champ noeuds sélectionnés reflète votre nouvelle sélection, et maintenant toutes les opérations sélectionnées ne seront effectuées que sur cet élément.

6. Dans le menu principal, sélectionnez l'option permettant de modifier les sous-réseaux du réseau Admin (option **3**).

7. Options au choix :

- Ajoutez un sous-réseau en saisissant la commande suivante : `add CIDR`
- Pour supprimer un sous-réseau, entrez la commande suivante : `del CIDR`
- Définissez la liste des sous-réseaux en saisissant la commande suivante : `set CIDR`



Pour toutes les commandes, vous pouvez entrer plusieurs adresses au format suivant : `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 à l'invite de saisie actuelle, puis les modifier si nécessaire.

L'exemple ci-dessous illustre l'ajout de sous-réseaux à la liste de sous-réseaux du réseau Admin :

```

Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

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

DK-10-224-5-20-G1
 10.0.0.0/8
 172.19.0.0/16
 172.21.0.0/16
 172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16

```

8. Lorsque vous êtes prêt, saisissez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.



Si vous avez sélectionné l'un des modes de sélection de nœuds « tous » à l'étape 3, appuyez sur **Entrée** (sans **q**) pour accéder au nœud suivant dans la liste.

9. Options au choix :

- Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple ci-dessous :

```

=====
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 en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions). **Note:** certains émulateurs de terminaux peuvent montrer des ajouts et des suppressions en utilisant le formatage barré.

Lorsque vous tentez de modifier la liste des sous-réseaux, le message suivant s'affiche :

CAUTION: The Admin Network subnet list on the node might contain /32 subnets derived from automatically applied routes that aren't persistent. Host routes (/32 subnets) are applied automatically if the IP addresses provided for external services such as NTP or DNS aren't reachable using default StorageGRID routing, but are reachable using a different interface and gateway. Making and applying changes to the subnet list will make all automatically applied subnets persistent. If you don't want that to happen, delete the unwanted subnets before applying changes. If you know that all /32 subnets in the list were added intentionally, you can ignore this caution.

Si vous n'avez pas spécifiquement affecté les sous-réseaux de serveurs NTP et DNS à un réseau, StorageGRID crée automatiquement une route hôte (/32) pour la connexion. Si, par exemple, vous préférez avoir une route /16 ou /24 pour la connexion sortante à un serveur DNS ou NTP, vous devez supprimer la route /32 créée automatiquement et ajouter les routes souhaitées. Si vous ne supprimez pas la route hôte créée automatiquement, elle sera conservée après que vous avez appliqué les modifications à la liste de sous-réseaux.



Bien que vous puissiez utiliser ces routes hôtes automatiquement découvertes, vous devez en général configurer manuellement les routes DNS et NTP pour assurer la connectivité.

10. Sélectionnez l'option **7** pour valider toutes les modifications échelonnée.

Cette validation garantit que les règles des réseaux Grid, Admin et client sont respectées, telles que l'utilisation de sous-réseaux redondants.

11. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications échelonnée et revenir ultérieurement pour continuer à effectuer les modifications.

Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les modifications non appliquées.

12. Effectuez l'une des opérations suivantes :

- Sélectionnez l'option **9** si vous souhaitez effacer toutes les modifications sans enregistrer ni appliquer la nouvelle configuration réseau.
- Sélectionnez l'option **10** si vous êtes prêt à appliquer des modifications et à provisionner la nouvelle configuration réseau. Pendant le provisionnement, le résultat affiche l'état au fur et à mesure que les mises à jour sont appliquées, comme indiqué dans l'exemple de résultat suivant :

Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name

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 pour le provisionnement.

14. Si vous avez autorisé l'accès SSH externe, "[bloquer l'accès](#)" lorsque vous avez terminé d'ajouter ou de modifier les listes de sous-réseaux.

Ajouter ou modifier les listes de sous-réseaux sur le réseau Grid dans StorageGRID

Vous pouvez utiliser l'outil Modifier IP pour ajouter ou modifier des sous-réseaux sur le réseau de grille.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux dans la liste de sous-réseaux du réseau de la grille. Les modifications affectent le routage sur tous les nœuds de la grille.



Si vous apportez uniquement des modifications à la liste de sous-réseaux du réseau Grid, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Dans le cas contraire, utilisez l'outil Modifier IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration du réseau ou si vous effectuez une modification du routage du réseau Grid et d'autres modifications du réseau simultanément.

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
- 192 168 130 121
- 192 168 131 101
- 192 168 131 121
- 192 168 130 102
- 192 168 130 122
- 192 168 131 102
- 192 168 131 122
- 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. L'accès SSH externe est bloqué par défaut. Si nécessaire, "[autoriser temporairement l'accès](#)".

2. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Démarrez l'outil Modifier IP en entrant la commande suivante : `change-ip`

4. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche.

```
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 l'option permettant de modifier les sous-réseaux du réseau Grid (option 4).



Les modifications apportées à la liste des sous-réseaux du réseau de la grille sont effectuées dans toute la grille.

6. Options au choix :

- Ajoutez un sous-réseau en saisissant la commande suivante : `add CIDR`
- Pour supprimer un sous-réseau, entrez la commande suivante : `del CIDR`
- Définissez la liste des sous-réseaux en saisissant la commande suivante : `set CIDR`



Pour toutes les commandes, vous pouvez entrer plusieurs adresses au format suivant : `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 à l'invite de saisie actuelle, puis les modifier si nécessaire.

L'exemple ci-dessous montre le paramétrage des sous-réseaux pour la liste de sous-réseaux du réseau Grid :

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
 172.16.0.0/21
 172.17.0.0/21
 172.18.0.0/21
 192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

7. Lorsque vous êtes prêt, saisissez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.
8. Options au choix :
 - Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple ci-dessous :

```
=====
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 en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré.

9. Sélectionnez l'option **7** pour valider toutes les modifications échelonnée.

Cette validation garantit que les règles des réseaux Grid, Admin et client sont respectées, telles que l'utilisation de sous-réseaux redondants.

10. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications échelonnée et revenir ultérieurement pour continuer à effectuer les modifications.

Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les

modifications non appliquées.

11. Effectuez l'une des opérations suivantes :

- Sélectionnez l'option **9** si vous souhaitez effacer toutes les modifications sans enregistrer ni appliquer la nouvelle configuration réseau.
- Sélectionnez l'option **10** si vous êtes prêt à appliquer des modifications et à provisionner la nouvelle configuration réseau. Pendant le provisionnement, le résultat affiche l'état au fur et à mesure que les mises à jour sont appliquées, comme indiqué dans l'exemple de résultat suivant :

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

12. Si vous avez sélectionné l'option **10** lors de la modification du réseau grille, sélectionnez l'une des options suivantes :

- **Appliquer** : appliquez les modifications immédiatement et redémarrez automatiquement chaque nœud si nécessaire.

Si la nouvelle configuration réseau fonctionnera simultanément avec l'ancienne configuration réseau sans aucune modification externe, vous pouvez utiliser l'option **appliquer** pour une modification de configuration entièrement automatisée.

- **Etape** : appliquez les modifications lors du prochain redémarrage des nœuds.

Si vous devez apporter des modifications de configuration de réseau physique ou virtuel pour que la nouvelle configuration de réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds affectés, effectuer les modifications de réseau physiques nécessaires et redémarrer les nœuds affectés.



Si vous utilisez l'option **stage**, redémarrez le nœud dès que possible après l'activation afin de minimiser les interruptions.

- **Annuler**: Ne faites pas de modifications de réseau pour le moment.

Si vous n'étiez pas conscient que les modifications proposées nécessitent de redémarrer les nœuds, vous pouvez reporter les modifications pour minimiser l'impact sur les utilisateurs. Si vous sélectionnez **annuler**, vous revenez au menu principal et les modifications sont préservées pour pouvoir 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.

13. Si la configuration est interrompue en raison d'erreurs, les options suivantes sont disponibles :

- Pour mettre fin à la procédure de modification IP et revenir au menu principal, entrez **a**.
- Pour réessayer l'opération qui a échoué, entrez **r**.
- Pour passer à l'opération suivante, saisissez **c**.

L'opération échouée peut être relancée ultérieurement en sélectionnant l'option **10** (appliquer les

modifications) dans le menu principal. La procédure de modification IP ne sera pas terminée tant que toutes les opérations n'auront pas été effectuées avec succès.

- Si vous avez dû intervenir manuellement (pour redémarrer un nœud, par exemple) et que l'action que l'outil pense avoir échoué a été réellement terminée, entrez **f** pour la marquer comme réussie et passer à l'opération suivante.

14. Téléchargez un nouveau package de récupération à partir du gestionnaire de grille.

- Sélectionnez **Maintenance > Système > Package de récupération**.
- Saisissez la phrase secrète pour le 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 du système StorageGRID .

15. Si vous avez autorisé l'accès SSH externe, "[bloquer l'accès](#)" lorsque vous avez terminé d'ajouter ou de modifier les listes de sous-réseaux.

Modifier les adresses IP de tous les nœuds dans une grille StorageGRID

Si vous devez modifier l'adresse IP du réseau Grid pour tous les nœuds de la grille, vous devez suivre cette procédure spéciale. Vous ne pouvez pas modifier l'adresse IP d'un réseau Grid Network à l'échelle de la grille en utilisant la procédure de modification de nœuds individuels.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Pour vous assurer que la grille démarre correctement, vous devez effectuer toutes les modifications en même temps.



Cette procédure s'applique uniquement au réseau Grid. Vous ne pouvez pas utiliser cette procédure pour modifier les adresses IP sur les réseaux Admin ou client.

Si vous souhaitez modifier les adresses IP et la MTU des nœuds sur un seul site, suivez les "[Modifier la configuration réseau du nœud](#)" instructions.

Étapes

1. Planifiez les modifications que vous devez apporter en dehors de l'outil Modifier l'IP, telles que les modifications apportées à DNS ou NTP, et les modifications apportées à la configuration SSO (Single Sign-On), si utilisée.



Si les serveurs NTP existants ne seront pas accessibles à la grille sur les nouvelles adresses IP, ajoutez les nouveaux serveurs NTP avant d'effectuer la procédure de modification ip.



Si les serveurs DNS existants ne seront pas accessibles à la grille sur les nouvelles adresses IP, ajoutez les nouveaux serveurs DNS avant d'effectuer la procédure de modification ip.



Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que des approbations de parties de confiance ont été configurées à l'aide d'adresses IP de nœuds 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. Reportez-vous à la configuration de l'authentification unique à l'aide de "OIDC" ou "SAML".



Si nécessaire, ajoutez le nouveau sous-réseau pour les nouvelles adresses IP.

2. L'accès SSH externe est bloqué par défaut. Si nécessaire, "[autoriser temporairement l'accès](#)".

3. Connectez-vous au nœud d'administration principal :

a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`

b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

4. Démarrez l'outil Modifier IP en entrant la commande suivante : `change-ip`

5. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche. Par défaut, le `Selected nodes` 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: █
```

6. Dans le menu principal, sélectionnez **2** pour modifier les informations IP/masque de sous-réseau, passerelle et MTU pour tous les nœuds.

a. Sélectionnez **1** pour modifier le réseau de grille.

Une fois votre sélection effectuée, l'invite affiche les noms des nœuds, le nom du réseau Grid, le type de données (IP/masque, passerelle ou MTU), et valeurs actuelles.

La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou de la MTU d'une interface configurée par DHCP changera l'interface en mode statique. Un avertissement s'affiche avant chaque interface configurée par DHCP.

Les interfaces configurées comme `fixed` ne peuvent pas être modifiées.

- a. Pour définir une nouvelle valeur, saisissez-la dans le format indiqué pour la valeur actuelle.
- b. Après avoir modifié tous les noeuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.

7. Vérifiez vos modifications en sélectionnant l'une des options suivantes :

- **5** : affiche les modifications dans la sortie isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en évidence en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie :

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- **6** : affiche les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré. L'affichage correct dépend de votre client terminal prenant en charge les séquences d'échappement VT100 nécessaires.

8. Sélectionnez l'option **7** pour valider toutes les modifications.

Cette validation garantit que les règles du réseau Grid, telles que l'absence de sous-réseaux se chevauchant, ne sont pas violées.

Dans cet exemple, la validation a renvoyé des erreurs.


```
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
```

9. Une fois la validation terminée, sélectionnez **10** pour appliquer la nouvelle configuration réseau.
10. Sélectionnez **stage** pour appliquer les modifications lors du prochain redémarrage des nœuds.



Vous devez sélectionner **étape**. N'effectuez pas de redémarrage en roulant, soit manuellement, soit en sélectionnant **Apply** au lieu de **stage** ; la grille ne démarrera pas correctement.

11. Une fois vos modifications terminées, sélectionnez **0** pour quitter l'outil Modifier IP.
12. Arrêtez tous les nœuds simultanément.



L'ensemble de la grille doit être arrêté, de sorte que tous les nœuds soient arrêtés en même temps.

13. Apportez les modifications nécessaires au réseau physique ou virtuel.
14. Vérifiez que tous les nœuds de la grille ne fonctionnent pas.
15. Mettez tous les nœuds sous tension.
16. Une fois la grille correctement mise en route :
 - a. Si vous avez ajouté des serveurs NTP, supprimez les anciennes valeurs du serveur NTP.
 - b. Si vous avez ajouté des serveurs DNS, supprimez les anciennes valeurs du serveur DNS.
17. Téléchargez le nouveau package de récupération à partir du gestionnaire de grille.
 - a. Sélectionnez **Maintenance > Système > Package de récupération**.
 - b. Saisissez la phrase secrète pour le provisionnement.
18. Si vous avez autorisé l'accès SSH externe, "**bloquer l'accès**" lorsque vous avez terminé de modifier les adresses IP.

Informations associées

- "[Ajouter ou modifier des listes de sous-réseaux sur le réseau Grid](#)"
- "[Arrêter le nœud de la grille](#)"

Ajoute des interfaces au nœud existant

Ajoutez des interfaces Admin ou Client à un nœud Linux dans StorageGRID

Procédez comme suit pour ajouter une interface sur le réseau Admin ou le réseau client à un nœud Linux après l'avoir installé.

Si vous n'avez pas configuré `ADMIN_NETWORK_TARGET` 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, voir ["Installer StorageGRID sur des nœuds logiciels"](#).

Cette procédure est effectuée sur le serveur Linux hébergeant le nœud nécessitant la nouvelle affectation de réseau, et non à l'intérieur du nœud. Cette procédure ajoute uniquement l'interface au nœud. Une erreur de validation se produit si vous tentez de spécifier d'autres paramètres réseau.

Pour fournir des informations d'adressage, vous devez utiliser l'outil Modifier IP. Voir ["Modifier la configuration réseau du nœud"](#).

Étapes

1. Connectez-vous au serveur Linux hébergeant le nœud.
2. Modifiez le fichier de configuration de nœud : `/etc/storagegrid/nodes/node-name.conf`.



Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produit.

- a. Ajouter une entrée pour la nouvelle cible réseau. Par exemple :

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Facultatif : ajoutez une entrée pour l'adresse MAC. Par exemple :

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Lancer la commande `node validate` :

```
sudo storagegrid node validate node-name
```

4. Résoudre toutes les erreurs de validation.

5. Lancer la commande `node reload` :

```
sudo storagegrid node reload node-name
```

Ajoutez des interfaces trunk ou d'accès à un nœud Linux dans StorageGRID

Vous pouvez ajouter une jonction ou des interfaces d'accès supplémentaires à un nœud Linux après l'avoir installé. Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

Avant de commencer

- Vous avez accès à la ["instructions pour l'installation de StorageGRID"](#) sur votre plateforme Linux.

- Vous avez le `Passwords.txt` fichier.
- Vous avez "autorisations d'accès spécifiques".



N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de restauration ou une procédure d'extension est active.

Description de la tâche

Procédez comme suit pour ajouter une ou plusieurs interfaces supplémentaires à un nœud Linux après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un nœud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

Le nœud est indisponible durant une brève ajout d'interfaces. Vous devez effectuer cette procédure sur un nœud à la fois.

Étapes

1. Connectez-vous au serveur Linux hébergeant le nœud.
2. À l'aide d'un éditeur de texte tel que vim ou pico, modifiez le fichier de configuration du nœud :

```
/etc/storagegrid/nodes/node-name.conf
```

3. Ajoutez une entrée au fichier pour spécifier le nom et, éventuellement, la description de chaque interface supplémentaire que vous souhaitez ajouter au nœud. Utilisez ce format.

```
INTERFACE_TARGET_nnnn=value
```

Pour *nnnn*, spécifiez un numéro unique pour chaque `INTERFACE_TARGET` entrée que vous ajoutez.

Pour *value*, spécifiez le nom de l'interface physique sur l'hôte bare-Metal. Ensuite, si vous le souhaitez, ajoutez une virgule et fournissez une description de l'interface, qui s'affiche sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

Par exemple :

```
INTERFACE_TARGET_0001=ens256, Trunk
```



Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produit.

4. Exécutez la commande suivante pour valider vos modifications dans le fichier de configuration du nœud :

```
sudo storagegrid node validate node-name
```

Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

5. Exécutez la commande suivante pour mettre à jour la configuration du nœud :

```
sudo storagegrid node reload node-name
```

Une fois que vous avez terminé

- Si vous avez ajouté une ou plusieurs interfaces de jonction, reportez-vous à ["Configurez les interfaces VLAN"](#) pour configurer une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent.
- Si vous avez ajouté une ou plusieurs interfaces d'accès, accédez à ["configurez les groupes haute disponibilité"](#) pour ajouter les nouvelles interfaces directement aux groupes haute disponibilité.

Ajoutez des interfaces trunk ou d'accès à un nœud VMware dans StorageGRID

Une fois le nœud installé, vous pouvez ajouter une jonction ou une interface d'accès à un nœud de machine virtuelle. Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

Avant de commencer

- Vous avez accès aux instructions pour ["Installation de StorageGRID sur votre plate-forme VMware"](#).
- Vous disposez des machines virtuelles VMware des nœuds d'administration et des nœuds de passerelle.
- Vous disposez d'un sous-réseau réseau qui n'est pas utilisé comme réseau, administrateur ou réseau client.
- Vous avez le `Passwords.txt` fichier.
- Vous avez ["autorisations d'accès spécifiques"](#).



N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de restauration ou une procédure d'extension est active.

Description de la tâche

Procédez comme suit pour ajouter une ou plusieurs interfaces supplémentaires à un nœud VMware après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un nœud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

Le nœud peut être indisponible durant une courte période lors de l'ajout d'interfaces.

Étapes

1. Dans vCenter, ajoutez une nouvelle carte réseau (de type VMXNET3) à un nœud d'administration et à une machine virtuelle de nœud de passerelle. Cochez les cases **connecté** et **se connecter à la mise sous tension**.

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. Utilisez `ip link show` pour confirmer que le nouveau sens256 d'interface réseau est détecté.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Une fois que vous avez terminé

- Si vous avez ajouté une ou plusieurs interfaces de jonction, reportez-vous à ["Configurez les interfaces VLAN"](#) pour configurer une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent.
- Si vous avez ajouté une ou plusieurs interfaces d'accès, accédez à ["configurez les groupes haute disponibilité"](#) pour ajouter les nouvelles interfaces directement aux groupes haute disponibilité.

Configurer les serveurs DNS dans StorageGRID

Vous pouvez ajouter, mettre à jour et supprimer des serveurs DNS, de sorte que vous puissiez utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP.

Pour utiliser des noms de domaine complets (FQDN) au lieu d'adresses IP lorsque vous spécifiez des noms d'hôte pour des destinations externes, spécifiez l'adresse IP de chaque serveur DNS que vous utiliserez. Ces entrées sont utilisées pour AutoSupport, les e-mails d'alerte, les notifications SNMP, les terminaux des services de plateforme, les pools de stockage cloud, et bien plus encore.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous disposez des adresses IP des serveurs DNS à configurer.

Description de la tâche

Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez,

"[Personnaliser la liste des serveurs DNS](#)" pour des nœuds individuels (généralement tous les nœuds d'un site), utiliser une configuration différente de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Ajouter un serveur DNS

Procédez comme suit pour ajouter un serveur DNS.

Étapes

1. Sélectionnez **Maintenance > Réseau > Serveurs DNS**.
2. Sélectionnez **Ajouter un autre serveur** pour ajouter un serveur DNS.
3. Sélectionnez **Enregistrer**.

Modifier un serveur DNS

Procédez comme suit pour modifier un serveur DNS.

Étapes

1. Sélectionnez **Maintenance > Réseau > Serveurs DNS**.
2. Sélectionnez l'adresse IP du nom du serveur que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.

Supprimer un serveur DNS

Procédez comme suit pour supprimer une adresse IP d'un serveur DNS.

Étapes

1. Sélectionnez **Maintenance > Réseau > Serveurs DNS**.
2. Sélectionnez l'icône de suppression  à côté de l'adresse IP.
3. Sélectionnez **Enregistrer**.

Modifier la configuration DNS pour un nœud StorageGRID 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. L'accès SSH externe est bloqué par défaut. Si nécessaire, "[autoriser temporairement l'accès](#)".
2. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`

b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

e. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`

f. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.

3. Connectez-vous au nœud que vous souhaitez mettre à jour avec une configuration DNS personnalisée :
`ssh node_IP_address`

4. 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``]

5. Ajoutez l'adresse IPv4 d'un serveur qui fournit un service de nom de domaine pour votre réseau : `add <nameserver IP_address>`
6. Répétez `add nameserver` la commande pour ajouter des serveurs de noms.
7. Suivez les instructions qui vous sont demandées pour d'autres commandes.
8. Enregistrez vos modifications et quittez l'application : `save`
9. Fermez le shell de commande sur le serveur : `exit`
10. Pour chaque nœud de grille, répétez les étapes de [connectez-vous au nœud](#) à [fermeture du shell de commande](#).

11. 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`
12. Si vous avez autorisé l'accès SSH externe, "[bloquer l'accès](#)" lorsque vous avez terminé de modifier la configuration DNS.

Gérer les serveurs NTP dans StorageGRID

Vous pouvez ajouter, mettre à jour ou supprimer des serveurs NTP (Network Time Protocol) pour vous assurer que les données sont synchronisées avec précision entre les nœuds de grid de votre système StorageGRID.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".
- Vous avez la phrase secrète pour le provisionnement.
- Vous disposez des adresses IPv4 des serveurs NTP à configurer.

Comment StorageGRID utilise-t-il le protocole NTP

Le système StorageGRID utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure entre tous les nœuds de la grille.

Le rôle NTP principal est attribué à chaque site au moins deux nœuds du système StorageGRID. Ils se synchronisent avec un minimum suggéré de quatre et un maximum de six sources de temps externes et entre elles. Chaque nœud du système StorageGRID qui n'est pas un nœud NTP principal agit comme un client NTP et se synchronise avec ces nœuds NTP primaires.

Les serveurs NTP externes se connectent aux nœuds auxquels vous avez précédemment attribué des rôles NTP principaux. C'est pourquoi il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.

Instructions relatives au serveur NTP

Suivez ces directives pour vous protéger contre les problèmes de synchronisation :

- Les serveurs NTP externes se connectent aux nœuds auxquels vous avez précédemment attribué des rôles NTP principaux. C'est pourquoi il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.
- Assurez-vous qu'au moins deux nœuds sur chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.
- Les serveurs NTP externes spécifiés doivent utiliser le protocole NTP. Vous devez spécifier les références de serveur NTP de Stratum 3 ou mieux pour éviter les problèmes de dérive du temps.



Lors de la spécification de la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, y compris StorageGRID. Pour plus de détails, consultez ["Limite de support pour une heure de haute précision"](#).

Configuration des serveurs NTP

Procédez comme suit pour ajouter, mettre à jour ou supprimer des serveurs NTP.

Étapes

1. Sélectionnez **Maintenance > Réseau > Serveurs NTP**.
2. Dans la section serveurs, ajoutez, mettez à jour ou supprimez des entrées de serveur NTP, si nécessaire.

Vous devez inclure au moins quatre serveurs NTP et vous pouvez spécifier jusqu'à six serveurs.

3. Entrez la phrase de passe de provisionnement pour votre système StorageGRID, puis sélectionnez **Enregistrer**.

La page est désactivée jusqu'à ce que les mises à jour de la configuration soient terminées.



Si tous vos serveurs NTP échouent au test de connexion après l'enregistrement des nouveaux serveurs NTP, ne poursuivez pas. Contactez l'assistance technique.

Résoudre les problèmes de serveur NTP

Si vous rencontrez des problèmes de stabilité ou de disponibilité des serveurs NTP initialement spécifiés lors de l'installation, vous pouvez mettre à jour la liste des sources NTP externes que le système StorageGRID utilise en ajoutant des serveurs supplémentaires ou en mettant à jour ou en supprimant des serveurs existants.

Rétablir la connectivité réseau pour les nœuds StorageGRID isolés

Dans certaines circonstances, un ou plusieurs groupes de nœuds peuvent ne pas être en mesure de contacter le reste de la grille. Par exemple, les modifications d'adresse IP à l'échelle du site ou de la grille peuvent entraîner l'isolement de nœuds.

Description de la tâche

L'isolation des nœuds est indiquée par :

- Alertes, telles que **Impossible de communiquer avec le nœud (alertes > actuel)**
- Diagnostics liés à la connectivité (**Support > Outils > Diagnostics**)

L'existence de nœuds isolés entraîne notamment les conséquences suivantes :

- Si plusieurs nœuds sont isolés, il se peut que vous ne puissiez pas vous connecter à ou accéder à Grid Manager.
- Si plusieurs nœuds sont isolés, les valeurs d'utilisation du stockage et de quota affichées sur le tableau de bord pour le gestionnaire de locataires peuvent être obsolètes. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

Pour résoudre le problème d'isolation, vous exécutez un utilitaire de ligne de commande sur chaque nœud isolé ou sur un nœud d'un groupe (tous les nœuds d'un sous-réseau ne contenant pas le 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 ou au groupe isolé de nœuds de contacter à nouveau toute la grille.



Si le système de noms de domaine multidiffusion (mDNS) est désactivé sur les réseaux, 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. Accédez au nœud et vérifiez `/var/local/log/dynip.log` la présence de messages d'isolation.

Par exemple :

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

Si vous utilisez la console VMware, un message indiquant que le nœud peut être isolé s'affiche.

Sur les déploiements Linux, des messages d'isolation apparaissent dans `/var/log/storagegrid/node/<nodename>.log` les fichiers.

2. Si les messages d'isolement sont récurrents et persistants, exécutez la commande suivante :

```
add_node_ip.py <address>
```

Où `<address>` est l'adresse IP d'un nœud distant connecté à la grille.

```
# /usr/sbin/add_node_ip.py 10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Vérifiez les éléments suivants pour chaque nœud précédemment isolé :

- Les services du nœud ont démarré.
- L'état du service IP dynamique est « en cours d'exécution » après l'exécution de la `storagegrid-status` commande.
- Sur la page nœuds, le nœud n'apparaît plus déconnecté du reste de la grille.



Si l'exécution de la `add_node_ip.py` commande ne résout pas le problème, d'autres problèmes de mise en réseau peuvent devoir être résolus.

Procédures d'hôte et de middleware

Migrer un nœud StorageGRID vers un nouvel hôte Linux

Vous pouvez migrer un ou plusieurs nœuds StorageGRID d'un hôte Linux (l' *hôte source*) vers un autre hôte Linux (l' *hôte cible*) pour effectuer la maintenance de l'hôte sans affecter les fonctionnalités ou la disponibilité de votre grille.

Par exemple, vous pouvez souhaiter migrer un nœud pour effectuer l'application de correctifs et le redémarrage du système d'exploitation.

Avant de commencer

- Vous avez planifié votre déploiement StorageGRID pour inclure la prise en charge de la migration. Voir ["Exigences de migration des conteneurs de nœuds"](#) .
- L'hôte cible est déjà prêt pour l'utilisation de StorageGRID.
- Le stockage partagé est utilisé pour tous les volumes de stockage par nœud
- Les interfaces réseau portent des noms cohérents sur tous les hôtes.



Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

D'autres types de nœuds, tels que les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur le même hôte. Toutefois, si vous avez plusieurs nœuds du même type (deux nœuds de passerelle, par exemple), n'installez pas toutes les instances sur le même hôte.

Nœud d'exportation à partir de l'hôte source

Dans un premier temps, arrêtez le nœud grid et exportez-le depuis l'hôte Linux source.

Exécutez les commandes suivantes sur l'hôte *source*.

Étapes

1. Obtenez l'état de tous les nœuds en cours d'exécution sur l'hôte source.

```
sudo storagegrid node status all
```

Exemple de résultat :

```
Name Config-State Run-State
DC1-ADM1 Configured Running
DC1-ARC1 Configured Running
DC1-GW1 Configured Running
DC1-S1 Configured Running
DC1-S2 Configured Running
DC1-S3 Configured Running
```

2. Identifiez le nom du nœud que vous souhaitez migrer et arrêtez-le si son état d'exécution est en cours d'exécution.

```
sudo storagegrid node stop DC1-S3
```

Exemple de résultat :

```
Stopping node DC1-S3
Waiting up to 630 seconds for node shutdown
```

3. Exportez le nœud depuis l'hôte source.

```
sudo storagegrid node export DC1-S3
```

Exemple de résultat :

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
want to import it again.
```

4. Notez la `import` commande suggérée dans le résultat.

Vous allez exécuter cette commande sur l'hôte cible à l'étape suivante.

Importer le nœud sur l'hôte cible

Après avoir exporté le nœud à partir de l'hôte source, vous importez et validez le nœud sur l'hôte cible. La validation confirme que le nœud a accès aux mêmes périphériques d'interface réseau et de stockage bloc que sur l'hôte source.

Exécutez les commandes suivantes sur l'hôte *cible*.

Étapes

1. Importez le nœud sur l'hôte cible.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Exemple de résultat :

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
You should run 'storagegrid node validate DC1-S3'
```

2. Valider la configuration de nœud sur le nouvel hôte.

```
sudo storagegrid node validate DC1-S3
```

Exemple de résultat :

```
Confirming existence of node DC1-S3... PASSED
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
DC1-S3... PASSED
Checking for duplication of unique values... PASSED
```

3. Si des erreurs de validation se produisent, traitez-les avant de démarrer le nœud migré.

Pour obtenir des informations de dépannage, consultez StorageGRID ["instructions d'installation"](#) pour votre système d'exploitation Linux.

Démarrer le nœud migré

Après avoir validé le nœud migré, vous démarrez le nœud en exécutant une commande sur l'hôte *cible*.

Étapes

1. Démarrez le nœud sur le nouvel hôte.

```
sudo storagegrid node start DC1-S3
```

2. Connectez-vous au Gestionnaire de grille et vérifiez que l'état du nœud est vert sans alerte.



La vérification de l'état du nœud est verte garantit que le nœud migré a redémarré et rejoint la grille. Si l'état n'est pas vert, ne migrez pas les nœuds supplémentaires pour que vous n'ayez plus d'un nœud hors service.

3. Si vous ne parvenez pas à accéder au Grid Manager, attendez 10 minutes, puis exécutez la commande suivante :

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

Vérifiez que l'état d'exécution du nœud migré est défini sur en cours d'exécution.

Configurer une machine virtuelle VMware pour un redémarrage automatique dans StorageGRID

Si la machine virtuelle ne redémarre pas après le redémarrage de l'hyperviseur VMware vSphere, vous devrez peut-être configurer la machine virtuelle pour le redémarrage automatique.

Cette procédure doit être effectuée si vous remarquez qu'une machine virtuelle ne redémarre pas lors de la récupération d'un nœud de la grille ou de l'exécution d'une autre procédure de maintenance.

Étapes

1. Dans l'arborescence du client VMware vSphere, sélectionnez la machine virtuelle qui n'a pas démarré.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Marche/Arrêt**.
3. Configurez l'hyperviseur VMware vSphere pour redémarrer automatiquement la machine virtuelle à l'avenir.

Récupérer ou remplacer des nœuds

Avertissements et considérations pour la récupération des nœuds StorageGRID

En cas de défaillance d'un nœud de la grille, vous devez le restaurer dès que possible. Avant de commencer, vous devez examiner tous les avertissements et considérations relatifs à la restauration du nœud.



StorageGRID est un système distribué composé de plusieurs nœuds qui travaillent les uns avec les autres. N'utilisez pas de snapshots de disque pour restaurer des nœuds de grille. Reportez-vous plutôt aux procédures de restauration et de maintenance pour chaque type de nœud.



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. ["Comment le support technique récupère un site"](#).

Voici quelques-unes des raisons pour lesquelles une restauration d'un nœud de grid a échoué dès que possible :

- Un nœud de grille défaillant peut réduire la redondance des données système et objet, ce qui vous rend vulnérable au risque de perte permanente de données en cas de défaillance d'un autre nœud.
- La défaillance d'un nœud de grid peut affecter l'efficacité des opérations quotidiennes.
- Un nœud de grid en panne peut vous permettre de surveiller les opérations système.
- Un nœud grid en panne peut entraîner une erreur de serveur interne 500 si des règles ILM strictes sont en place.
- Si un nœud de la grille n'est pas restauré rapidement, le temps de restauration peut augmenter. Par exemple, des files d'attente peuvent se développer et doivent être effacées avant la fin de la restauration.

Suivez toujours la procédure de restauration pour le type spécifique de nœud de grille que vous restaurez. Les procédures de restauration varient en fonction des nœuds d'administration primaires ou non primaires, des nœuds de passerelle, des nœuds d'appliance et des nœuds de stockage.

Conditions préalables à la récupération des nœuds de la grille

Les conditions suivantes sont réunies lors de la récupération des nœuds de la grille :

- Le matériel physique ou virtuel en panne a été remplacé et configuré.
- La version du programme d'installation de l'appliance StorageGRID installée sur l'appliance de remplacement correspond à la version logicielle de votre système StorageGRID, comme décrit à la section ["Vérifiez et mettez à niveau la version du programme d'installation de l'appliance StorageGRID"](#).
- Si vous récupérez un nœud de grille autre que le nœud d'administration principal, une connectivité doit exister entre le nœud de grille en cours de récupération et le nœud d'administration gérant la procédure de récupération.
- 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 restauration de nœud en cas de défaillance d'un serveur hébergeant plusieurs nœuds de la grille

Si un serveur hébergeant plusieurs nœuds de grille tombe en panne, vous pouvez restaurer les nœuds dans n'importe quel ordre. Cependant, si le serveur défaillant héberge le nœud d'administration principal et qu'aucun nœud d'administration non principal n'existe, vous devez restaurer le nœud d'administration principal en premier.

Adresses IP des nœuds restaurés

N'essayez pas de restaurer un nœud à l'aide d'une adresse IP actuellement attribuée à un autre nœud. Lorsque vous déployez le nouveau nœud, utilisez l'adresse IP actuelle du nœud défaillant ou une adresse IP non utilisée.

Si vous utilisez une nouvelle adresse IP pour déployer le nouveau nœud puis restaurer le nœud, la nouvelle adresse IP continuera à être utilisée pour le nœud restauré. Si vous souhaitez revenir à l'adresse IP d'origine, utilisez l'outil Modifier l'adresse IP une fois la restauration terminée.

Rassemblez les matériaux nécessaires pour la récupération des nœuds de la grille StorageGRID

Avant d'effectuer des procédures de maintenance, vous devez vous assurer que vous disposez des matériaux nécessaires pour récupérer un nœud de grille défaillant.

Élément	Remarques
Archive de l'installation de StorageGRID	Si vous avez besoin de restaurer un nœud grid, vous devez vous en remettre Téléchargez les fichiers d'installation de StorageGRID à votre plateforme. Remarque : vous n'avez pas besoin de télécharger des fichiers si vous récupérez des volumes de stockage défectueux sur un nœud de stockage.
L'ordinateur portable de service	L'ordinateur portable de service doit être équipé des éléments suivants : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"

Élément	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. Lorsque vous êtes connecté à un nœud d'administration, utilisez le gestionnaire de grille pour télécharger un package de récupération. Sélectionnez Maintenance > Système > Package de récupération. Si vous ne pouvez pas accéder au gestionnaire de grille, 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 fichier	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le forfait de récupération.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement ne se trouve pas dans Passwords.txt le fichier.
Documentation actuelle pour votre plate-forme	Rendez-vous sur le site Web du fournisseur de la plate-forme pour obtenir de la documentation. Pour connaître les versions de votre plate-forme actuellement prises en charge, consultez le "Matrice d'interopérabilité NetApp".

Téléchargez et extrayez les fichiers d'installation StorageGRID

Téléchargez le logiciel et extrayez les fichiers, sauf si vous êtes "[Récupération des volumes de stockage défectueux sur un noeud de stockage](#)".

Vous devez utiliser la version de StorageGRID en cours d'exécution sur la grille.

Étapes

1. Déterminez quelle version du logiciel est actuellement installée. Dans la partie supérieure du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **About**.
2. Accédez à la "[Page de téléchargements NetApp pour StorageGRID](#)".
3. Sélectionnez la version de StorageGRID en cours d'exécution sur la grille.

Les versions du logiciel StorageGRID ont ce format : 11.x.y.

4. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
6. Dans la colonne **Install StorageGRID** de la page de téléchargement, sélectionnez le .tgz fichier ou .zip pour votre plate-forme.

La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installé.

Utilisez le .zip fichier si vous exécutez Windows.

Plateforme	Archive d'installation
RHEL	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

7. Téléchargez et extrayez le fichier d'archive.
8. Accédez à la section 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.

9. Si vous récupérez un "nœud basé sur un logiciel", sélectionnez les fichiers appropriés :

RHEL

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Progiciel RPM pour l'installation des images de nœud StorageGRID sur vos hôtes RHEL.
	Progiciel RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle Ansible et de manuel de vente pour la configuration des hôtes RHEL pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Ubuntu ou Debian

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.

Chemin d'accès et nom de fichier	Description
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

VMware

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.

Chemin d'accès et nom de fichier	Description
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Le fichier modèle Open Virtualization format (.ovf) et le fichier manifeste (.mf) pour le déploiement du nœud d'administration principal.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement de nœuds Admin non primaires.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de passerelle.
	Le fichier modèle (.ovf) et le fichier manifeste (.mf) pour le déploiement des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> script.
	Fichier de configuration vide à utiliser avec le <code>configure-storagegrid.py</code> script.

Chemin d'accès et nom de fichier	Description
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le script Python associé <code>storagegrid-ssoauth-azure.py</code> pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. Remarque : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

10. Si vous récupérez un système basé sur l'appliance StorageGRID, sélectionnez les fichiers appropriés.



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 où vous effectuez la procédure de récupération.

Chemin d'accès et nom de fichier	Description
	DEB package pour l'installation des images de nœud StorageGRID sur vos appareils.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .

Sélectionnez la procédure de récupération du nœud StorageGRID

Sélectionnez la procédure de récupération appropriée au type de nœud qui a échoué.

Nœud de grille	Procédure de reprise
Nœud de stockage	La procédure de récupération du nœud de stockage dépend du type de panne. "Restaurez les données après une panne de nœud de stockage"
Nœud d'administration	La procédure nœud d'administration varie selon que vous devez restaurer le nœud d'administration principal ou un nœud d'administration non primaire. "Restaurez vos données après une panne de nœud d'administration"
Nœud de passerelle	"Restaurez les données à partir d'une défaillance de nœud de passerelle"
Nœud d'archivage	"Restauration suite aux défaillances de nœud d'archivage (site de documentation StorageGRID 11.8)"



Si un serveur hébergeant plusieurs nœuds de grille tombe en panne, vous pouvez restaurer les nœuds dans n'importe quel ordre. Cependant, si le serveur défaillant héberge le nœud d'administration principal et qu'aucun nœud d'administration non principal n'existe, vous devez d'abord restaurer le nœud d'administration principal. Restaurer d'abord le nœud d'administration principal empêche les autres restaurations de nœuds d'être bloquées lorsqu'elles tentent de contacter le nœud d'administration principal. Si un nœud d'administration non principal est disponible, vous pouvez également l'utiliser pour restaurer d'autres nœuds afin que ces restaurations puissent se poursuivre sans contacter le nœud d'administration principal.

Restaurez les données après une panne de nœud de stockage

Récupérer après des pannes de nœuds de stockage StorageGRID

La procédure de récupération d'un nœud de stockage défaillant dépend du type de panne et du type de nœud de stockage qui a échoué.

Utilisez ce tableau pour sélectionner la procédure de restauration d'un nœud de stockage défaillant.

Problème	Action	Remarques
Plusieurs nœuds de stockage ont échoué.	Contactez l'assistance technique.	En cas de défaillance de plusieurs nœuds de stockage, l'assistance technique doit intervenir pour la récupération afin d'éviter les incohérences de la base de données Cassandra susceptibles d'entraîner une perte de données. Une procédure de restauration du site peut s'avérer nécessaire. Le support technique peut déterminer à quel moment il est sûr de commencer la récupération d'un deuxième nœud de stockage. Remarque : Si plusieurs nœuds de stockage contenant le service ADC tombent en panne sur un site, toutes les demandes de service de plateforme en attente pour ce site seront perdues.
Plusieurs nœuds de stockage sur un site ont échoué ou l'ensemble d'un site a échoué.	Contactez l'assistance technique. Il peut être nécessaire d'effectuer une procédure de reprise sur site.	L'assistance technique évaluera votre situation et élaborera un plan de reprise. Voir " Comment le support technique récupère un site ".
Un nœud de stockage de l'appliance est défectueux.	" Restaurez le nœud de stockage de l'appliance "	La procédure de restauration des nœuds de stockage de l'appliance est la même pour toutes les défaillances.
Un ou plusieurs volumes de stockage sont en panne, mais le lecteur système est intact	" Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact "	Cette procédure est utilisée pour les nœuds de stockage basés sur logiciel.
Le lecteur système est défectueux.	" Restaurez les données après une panne de disque système "	La procédure de remplacement des nœuds dépend de la plateforme de déploiement et indique si des volumes de stockage sont également défectueux.



Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être une sortie de script mentionnant « Reaper » ou « Cassandra repair ». Si un message d'erreur s'affiche, indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

Restaurez le nœud de stockage de l'appliance

Avertissements pour la récupération des nœuds de stockage StorageGRID de l'appliance StorageGRID

La procédure de restauration d'un nœud de stockage de l'appliance StorageGRID défaillant est identique, que vous soyez en train de récupérer à partir de la perte du disque système ou de la perte de volumes de stockage uniquement.



Si plusieurs nœuds de stockage sont en panne (ou sont hors ligne), contactez le support technique. N'exécutez pas la procédure de récupération suivante. Une perte de données pourrait survenir. Pour plus d'informations, reportez-vous à ["Comment le support technique récupère un site"](#).



Si les règles ILM sont configurées pour ne stocker qu'une seule copie répliquée, et si cette copie existe sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.



Pour connaître les procédures de maintenance du matériel, telles que les instructions de remplacement d'un contrôleur ou de réinstallation de SANtricity OS, reportez-vous au ["instructions d'entretien pour votre appareil de stockage"](#).

Préparer le nœud de stockage StorageGRID pour la réinstallation

Lors de la restauration d'un nœud de stockage d'appliance, vous devez d'abord préparer l'appliance pour la réinstallation du logiciel StorageGRID.

Étapes

1. Connectez-vous au nœud de stockage défaillant :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Préparez le nœud de stockage de l'appliance pour l'installation du logiciel StorageGRID. `sgareinstall`

3. Lorsque vous êtes invité à continuer, entrez : `y`

L'appliance redémarre et votre session SSH se termine. La disponibilité du programme d'installation de l'appliance StorageGRID prend généralement 5 minutes environ, même si dans certains cas, vous devrez attendre jusqu'à 30 minutes.



N'essayez pas d'accélérer le redémarrage en mettant l'appareil hors tension ou en le réinitialisant autrement. Vous pouvez interrompre les mises à niveau automatiques du BIOS, du contrôleur BMC ou d'autres micrologiciels.

Le nœud de stockage de l'appliance StorageGRID est réinitialisé et les données du nœud de stockage ne sont plus accessibles. Les adresses IP configurées pendant le processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cette opération une fois la procédure terminée.

Une fois la commande exécutée `sgareinstall`, tous les comptes, mots de passe et clés SSH provisionnés par StorageGRID sont supprimés et de nouvelles clés hôte sont générées.

Démarrez l'installation de l'appliance StorageGRID

Pour installer StorageGRID sur un nœud de stockage de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID, qui est inclus sur l'appliance.

Avant de commencer

- L'appliance a été installée dans un rack, connectée à vos réseaux et sous tension.
- Les liens réseau et les adresses IP ont été configurés pour l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.
- Vous connaissez l'adresse IP de l'un des nœuds d'administration suivants :
 - Le nœud d'administration principal de la grille StorageGRID
 - Un nœud d'administration non principal, si disponible
- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.
- Vous avez terminé ces tâches préalables en suivant les instructions d'installation de votre appliance de stockage. Voir "[Démarrage rapide pour l'installation du matériel](#)".
- Vous utilisez un "[navigateur web pris en charge](#)".
- Vous connaissez l'une des adresses IP attribuées au contrôleur de calcul dans l'appliance. Vous pouvez utiliser l'adresse IP du réseau d'administration (port de gestion 1 sur le contrôleur), du réseau Grid ou du réseau client.

Description de la tâche

Pour installer StorageGRID sur un nœud de stockage d'appliance :

- Vous indiquez l'adresse IP du nœud d'administration principal. Si le nœud d'administration principal est indisponible, vous indiquez l'adresse IP du nœud d'administration non principal, si disponible. Vous confirmez également le nom d'hôte (nom 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.

- Partway tout au long du processus, l'installation se met en pause. Pour reprendre l'installation, vous devez vous connecter à Grid Manager et configurer le nœud de stockage en attente en remplacement du nœud défaillant.
- Une fois le nœud configuré, le processus d'installation de l'appliance est terminé et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

```
https://Controller_IP:8443
```

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section connexion au 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 détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Étapes
Entrée IP manuelle	a. Décochez la case Activer la découverte du nœud d'administration. b. Saisissez manuellement l'adresse IP. Remarque : pour l'installation, saisissez manuellement l'adresse IP du nœud d'administration que vous souhaitez utiliser pour installer le nœud. Pour la récupération, utilisez l'adresse IP du nœud d'administration principal si disponible ; sinon, utilisez l'adresse IP d'un nœud d'administration non principal. a. Sélectionnez Enregistrer. b. Patientez pendant que l'état de connexion de la nouvelle adresse IP devient « prêt ».
Détection 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 de la grille sur laquelle ce nœud de stockage d'appliance sera déployé. Remarque : pour la récupération, utilisez l'adresse IP du nœud d'administration principal si disponible ; sinon, utilisez l'adresse IP d'un nœud d'administration non principal. a. Sélectionnez Enregistrer. b. Patientez pendant que l'état de connexion de la nouvelle adresse IP devient « prêt ».

4. Dans le champ **Nom du nœud**, saisissez le même nom d'hôte (nom du système) que celui utilisé pour le nœud que vous récupérez, puis sélectionnez **Enregistrer**.
5. Dans la section Installation, vérifiez 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 **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

6. Depuis la page d'accueil de l'installateur d'appliance StorageGRID, sélectionnez **Démarrer l'installation**.

L'état actuel passe à « Installation en cours », et la page d'installation du moniteur s'affiche.



Si vous devez accéder manuellement à la page d'installation de Monitor, sélectionnez **Monitor installation** dans la barre de menu. Voir "[Surveiller l'installation de l'appareil](#)".

Surveillez l'installation de l'appliance StorageGRID

Le programme d'installation de l'appliance StorageGRID indique l'état jusqu'à ce que l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appliance est redémarrée.

Étapes

1. Pour suivre la progression de l'installation, sélectionnez **Monitor installation** dans la barre de menu.

La page d'installation de Monitor affiche la progression de l'installation.

La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.



Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état « ignoré ».

2. Passez en revue l'état d'avancement des deux premières étapes d'installation.

- **1. Configurer le stockage**

Au cours de cette étape, le programme d'installation se connecte au contrôleur de stockage, efface toute configuration existante, communique avec SANtricity OS pour configurer des volumes et configure les paramètres de l'hôte.

- **2. Installez OS**

Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'appliance.

3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'étape **installer StorageGRID** s'arrête et un message s'affiche sur la console intégrée vous invitant à approuver ce nœud sur le nœud d'administration à l'aide du gestionnaire de grille.

4. Allez à "[Sélectionnez Démarrer la restauration pour configurer le nœud de stockage de l'appliance](#)".

Sélectionnez Démarrer la récupération pour configurer le nœud de stockage de l'appliance StorageGRID

Vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer un nœud de stockage d'appliance en remplacement du nœud défaillant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".

- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé un nœud de stockage d'appliance de restauration.
- Vous disposez de la date de début des travaux de réparation pour les données avec code d'effacement.

Étapes

1. Dans le Grid Manager, sélectionnez **Maintenance > Tasks > Node recovery**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la **phrase secrète de provisionnement**.
4. Sélectionnez **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 Q				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.
 - Si le nœud de la grille atteint l'étape « En attente d'étapes manuelles », vous devez "[Remontez et reformatez manuellement les volumes de stockage de l'appliance](#)".
 - Si le message « En attente d'étapes manuelles » n'apparaît pas, cela signifie que les volumes de stockage ont été automatiquement remontés et reformatés, et que vous pouvez "[restaurer les données d'objet sur les volumes](#)".



À tout moment pendant la récupération, vous pouvez sélectionner **Réinitialiser** pour lancer une nouvelle récupération. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.

Si vous souhaitez réessayer la restauration après la réinitialisation de la procédure, vous devez restaurer le nœud de l'appliance à l'état pré-installé en exécutant `sgareinstall` sur le nœud.

Remonter et reformater les volumes de stockage de l'appliance StorageGRID (étapes manuelles)

Si la procédure automatique ne parvient pas à remonter les volumes de stockage préservés et à reformater les volumes de stockage défaillants, vous devez exécuter manuellement deux scripts pour effectuer ces opérations. Le premier script remonte les volumes correctement formatés en tant que volumes de stockage StorageGRID. Le second script reformate les volumes non montés, reconstruit la base de données Cassandra si nécessaire et démarre les services.

Lors de la récupération d'un nœud de stockage, si le message « En attente d'instructions manuelles » s'affiche dans le Gestionnaire de grille, suivez ces étapes pour remonter et reformater les volumes de stockage. Si ce message ne s'affiche pas, les opérations de remontage et de reformatage se sont terminées automatiquement, et vous pouvez ignorer *cette* procédure et "[restaurer les données de l'objet](#)".

Avant de commencer

- Vous avez déjà remplacé le matériel de tous les volumes de stockage défectueux que vous savez avoir besoin d'être remplacé.

L'exécution `sn-remount-volumes` du script peut vous aider à identifier d'autres volumes de stockage 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. Ne courez pas le `sn-recovery-postinstall.sh` scénario.

Description de la tâche

Pour effectuer cette procédure, vous devez effectuer les tâches de haut niveau suivantes :

- Connectez-vous au nœud de stockage récupéré.
- Exécutez `sn-remount-volumes` le script pour remonter les volumes de stockage correctement formatés. Lorsque ce script s'exécute, il effectue les opérations suivantes :
 - Monte et démonte chaque volume de stockage pour relire le journal XFS.
 - Effectue une vérification de cohérence de fichier XFS.
 - Si le système de fichiers est cohérent, détermine si le volume de stockage est un volume de stockage StorageGRID correctement formaté.
 - Si le volume de stockage est correctement formaté, remonter le volume de stockage. Toutes les données existantes du volume restent intactes.
- Examinez la sortie du script et résolvez tout problème.
- Exécutez `sn-recovery-postinstall.sh` le script. Lorsque ce script s'exécute, il effectue les opérations suivantes :



Ne redémarrez pas un nœud de stockage pendant la restauration avant de l'exécuter `sn-recovery-postinstall.sh` (étape 4) pour reformater les volumes de stockage défectueux et restaurer les métadonnées de l'objet. Le redémarrage du nœud de stockage avant la `sn-recovery-postinstall.sh` fin de entraîne des erreurs pour les services qui tentent de démarrer et provoque la sortie du mode de maintenance par les nœuds d'appliance StorageGRID.

- Reformate les volumes de stockage que le script n'a pas pu monter ou dont le `sn-remount-volumes` formatage a été incorrect.



Lorsqu'un volume de stockage est reformaté, toutes les données de ce volume sont perdues. Vous devez effectuer une procédure supplémentaire pour restaurer les données d'objet à partir d'autres emplacements de la grille, en supposant que les règles ILM ont été configurées pour stocker plusieurs copies d'objet.

- 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 :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez le premier script pour remonter tous les volumes de stockage correctement formatés.



Si tous les volumes de stockage sont nouveaux et doivent être formatés, ou si tous les volumes de stockage ont échoué, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage démontés.

- a. Exécutez le script : `sn-remount-volumes`

Ce script peut prendre des heures sur les volumes de stockage qui contiennent des données.

- b. Au fur et à mesure de l'exécution du script, vérifiez le résultat et répondez aux invites.



Si nécessaire, vous pouvez utiliser `tail -f` la commande pour contrôler le contenu du fichier journal du script (`/var/local/log/sn-remount-volumes.log`) . Le fichier journal contient des informations plus détaillées que la sortie de la ligne de commande.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
```



```

Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID 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 ont rencontré des erreurs.

- /dev/sdb La vérification de la cohérence du système de fichiers XFS a été effectuée et la structure de volume était valide. Le montage a donc réussi. Les données sur les périphériques 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 impossible de monter car le disque n'a pas été initialisé ou le superbloc du disque a été corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter le contrôle de cohérence du système de fichiers.
 - Si le volume de stockage est relié à un nouveau disque, répondez **N** à l'invite. Vous n'avez pas besoin de vérifier le système de fichiers sur un nouveau disque.
 - Si le volume de stockage est relié à un disque existant, répondez **y** à l'invite. Vous pouvez utiliser les résultats de la vérification du système de fichiers pour déterminer la source de la corruption. Les résultats sont enregistrés dans le /var/local/log/sn-remount-volumes.log fichier journal.
- /dev/sde Le contrôle de cohérence du système de fichiers XFS a été effectué et la structure de volume était valide. Cependant, l'ID de nœud LDR dans le volID fichier ne correspond pas à l'ID de ce nœud de stockage (`configured LDR noid` affiché en haut). Ce message indique que ce volume appartient à un autre nœud de stockage.

3. Examinez la sortie du script et résolvez tout problème.



Si un volume de stockage a échoué au contrôle de cohérence du système de fichiers XFS ou ne peut pas être monté, vérifiez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution `sn-recovery-postinstall.sh` du script sur ces volumes.

- a. Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si aucun volume n'est répertorié, exécutez à nouveau le script.
- b. Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a pas d'erreur indiquant qu'un volume de stockage n'appartient pas à ce nœud de stockage.

Dans l'exemple, la sortie de `/dev/sde` inclut le message d'erreur suivant :

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Si un volume de stockage est signalé comme appartenant à un autre nœud de stockage, contactez le support technique. Si vous exécutez `sn-recovery-postinstall.sh` le script, le volume de stockage sera reformaté, ce qui pourrait entraîner une perte de données.

- c. Si aucun périphérique de stockage n'a pu être monté, notez le nom du périphérique et réparez ou remplacez le périphérique.



Vous devez réparer ou remplacer tout périphérique de stockage qui n'a pas pu être monté.

- d. Après avoir réparé ou remplacé tous les périphériques unmountable, exécutez à nouveau le `sn-remount-volumes` script pour confirmer que tous les volumes de stockage pouvant être remontés ont été remontés.



Si un volume de stockage ne peut pas être monté ou est mal formaté et que vous passez à l'étape suivante, le volume et toutes les données du volume seront supprimés. Si vous aviez deux copies de vos données d'objet, vous n'aurez qu'une seule copie jusqu'à la fin de la procédure suivante (restauration des données d'objet).



N'exécutez pas `sn-recovery-postinstall.sh` le script si vous pensez que les données restantes sur un volume de stockage défaillant ne peuvent pas être reconstruites à partir d'un autre emplacement de la grille (par exemple, si votre règle 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 savoir comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` script : `sn-recovery-postinstall.sh`

Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui n'ont pas été correctement formatés. Reconstitue la base de données Cassandra sur le nœud, si nécessaire, et démarre les services sur le nœud de stockage.

Gardez à l'esprit les points suivants :

- L'exécution du script peut prendre des heures.
- En général, vous devez laisser la session SSH seule pendant que le script est en cours d'exécution.
- N'appuyez pas sur **Ctrl+C** lorsque la session SSH est active.
- Le script s'exécute en arrière-plan en cas d'interruption du réseau et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page récupération.
- Si le nœud de stockage utilise le service RSM, le script peut sembler bloqué pendant 5 minutes au redémarrage des services de nœud. Ce délai de 5 minutes est prévu lorsque l'entretien du RSM démarre pour la première fois.



Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.



Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être une sortie de script mentionnant « Reaper » ou « Cassandra repair ». Si un message d'erreur s'affiche, indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

5. Pendant l'`sn-recovery-postinstall.sh` exécution du script, surveillez la page récupération dans le Gestionnaire de grille.

La barre de progression et la colonne Stage de la page récupération fournissent un état de haut niveau du `sn-recovery-postinstall.sh` script.

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. Une fois que le `sn-recovery-postinstall.sh` script a démarré les services sur le nœud, vous pouvez restaurer les données d'objet sur tous les volumes de stockage formatés par le script.

Le script vous demande si vous souhaitez utiliser le processus de restauration de volume de Grid Manager pour restaurer les données des objets.

- Dans la plupart des cas, vous devriez "[Restaurez les données d'objet à l'aide de Grid Manager](#)". Répondez `y` pour utiliser le Gestionnaire de grille.
- Dans de rares cas, par exemple si le nœud de remplacement dispose de moins de volumes disponibles pour le stockage d'objets que le nœud d'origine, contactez le support technique pour

restaurer manuellement les données d'objets. Si l'un de ces cas s'applique, répondez n et appuyez sur n'importe quelle touche pour revenir à la ligne de commandes.

Restaurez les données d'objet sur un volume de stockage pour une StorageGRID appliance

Après avoir restauré des volumes de stockage pour le nœud de stockage de l'appliance, vous pouvez restaurer les données d'objet répliquées ou avec code d'effacement qui ont été perdues en cas de défaillance du nœud de stockage.

Avant de commencer

- Si la procédure automatique n'a pas permis de remonter les volumes de stockage préservés et de reformater les volumes de stockage défaillants, vous avez effectué l'une des procédures suivantes :
 - ["Remontage et reformatage des volumes de stockage de l'appliance \(étapes manuelles\)"](#)
 - ["Remontage et reformatage des volumes de stockage \(étapes manuelles\)"](#)
- Vous avez confirmé que le nœud de stockage sur lequel vous restaurez des objets a un état de connexion **Connecté**  sur l'onglet **Nœuds** > **Vue d'ensemble** dans le Grid Manager.
- Vous avez confirmé ce qui suit :
 - L'extension de la grille pour ajouter un nœud de stockage n'est pas en cours.
 - La mise hors service d'un nœud de stockage n'est pas en cours ni échouée.
 - La récupération d'un volume de stockage défaillant n'est pas en cours.
 - La récupération d'un nœud de stockage dont le disque système est défaillant n'est pas en cours.
 - Aucune opération de rééquilibrage de l'EC n'est en cours.
 - Le clonage des nœuds d'appliance n'est pas en cours.

Description de la tâche

Une fois les disques remplacés et les volumes formatés, Grid Manager affiche les volumes comme candidats à la restauration dans l'onglet **Maintenance** > **Restauration de volume** > **Nœuds à restaurer**.

Lorsque cela est possible, restaurez les données d'objet à l'aide de la page Restauration des volumes du Gestionnaire de grille. Vous pouvez soit [activer le mode de restauration automatique](#) lancer automatiquement la restauration du volume lorsque les volumes sont prêts à être restaurés, soit [effectuez manuellement la restauration des volumes](#). Suivez ces instructions :

- 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 sont en panne, mais pas tous
 - Tous les volumes de stockage d'un nœud sont en panne et sont remplacés par le même nombre de volumes ou plus

La page de restauration de volume dans le gestionnaire de grille vous permet également de [surveiller le processus de restauration des volumes](#) et [afficher l'historique de restauration](#).

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, contactez le support technique pour obtenir de l'aide.

Vous pouvez restaurer deux types de données d'objet :

- Les objets de données répliqués sont restaurés à partir d'autres emplacements, dans la mesure où les règles ILM de la grille ont été configurées de façon à rendre disponibles les copies objet.
 - Si une règle ILM a été configurée pour ne stocker qu'une seule copie répliquée et que cette copie se trouvait 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 demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet.
- Les objets de données avec code d'effacement (EC) sont restaurés en réassemblez les fragments stockés. Les fragments corrompus ou perdus sont recréés par l'algorithme de code d'effacement à partir des fragments de données et de parité restants.

Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.



La restauration des volumes dépend de la disponibilité des ressources dans lesquelles les copies objet sont stockées. La progression de la restauration des volumes n'est pas linéaire et peut prendre des jours ou des semaines.

Active le mode de restauration automatique

Lorsque vous activez le mode de restauration automatique, la restauration des volumes 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 activé.
3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails.



- Vous ne pourrez pas lancer manuellement de tâches de restauration de volume sur aucun nœud.
- Les restaurations de volume ne démarrent automatiquement que lorsqu'aucune autre procédure de maintenance n'est en cours.
- Vous pouvez contrôler l'état du travail à partir de la page de surveillance de la progression.
- StorageGRID relance automatiquement les restaurations de volume qui ne démarrent pas.

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.

[[restauration manuelle]] restaurez manuellement un volume ou un nœud défaillant

Procédez comme suit 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 de **mode de restauration automatique** sur la position Désactivé.

Le numéro de l'onglet indique le nombre de nœuds pour lesquels des volumes nécessitent une restauration.

3. Développez chaque nœud pour afficher les volumes qui nécessitent une restauration, ainsi que leur état.
4. Corrigez tous les problèmes empêchant la restauration de chaque volume. Les problèmes sont indiqués lorsque vous sélectionnez **en attente d'étapes manuelles**, s'il s'affiche comme état du volume.
5. Sélectionnez un nœud à restaurer où tous les volumes indiquent l'état prêt pour la restauration.

Vous ne pouvez restaurer les volumes que pour un nœud à la fois.

Chaque volume du nœud doit indiquer qu'il est prêt à être restauré.

6. Sélectionnez **Démarrer la restauration**.
7. Réglez les avertissements qui peuvent apparaître ou sélectionnez **Démarrer malgré tout** pour ignorer les avertissements et lancer la restauration.

Les nœuds sont déplacés de l'onglet **nœuds à restaurer** vers l'onglet **progression de la restauration** au démarrage de la restauration.

Si une restauration de volume ne peut pas être démarrée, le nœud revient à l'onglet **nœuds à restaurer**.

Afficher la progression de la restauration

L'onglet **progression de la restauration** affiche l'état du processus de restauration du volume et des informations sur les volumes d'un nœud restauré.

Les taux de réparation des données pour les objets répliqués et ceux dont le codage d'effacement est utilisé dans tous les volumes correspondent à des moyennes résumant toutes les restaurations en cours. Le pourcentage d'objets dans ces volumes qui sont intacts et ne nécessitent aucune restauration est également indiqué.



La restauration des données répliquées dépend de la disponibilité des ressources dans lesquelles les copies répliquées sont stockées. La progression de la restauration des données répliquées n'est pas linéaire et peut prendre des jours ou des semaines.

La section tâches de restauration affiche des informations sur les restaurations de volume démarrées à partir du Gestionnaire de grille.

- Le nombre indiqué dans l'en-tête de la section travaux de restauration indique le nombre de volumes en cours de restauration ou en file d'attente de restauration.
- Le tableau affiche des informations sur chaque volume d'un nœud en cours de restauration ainsi que sa progression.
 - La progression de chaque nœud affiche le pourcentage pour chaque travail.
 - Développez la colonne Détails pour afficher l'heure de début de la restauration et l'ID du travail.
- En cas d'échec de la restauration d'un volume :

- La colonne **État** indique `failed (attempting retry)`, et sera réexécutée automatiquement.
- Si plusieurs travaux de restauration ont échoué, le travail le plus récent sera automatiquement repassé en premier.
- L'alerte **EC repair failure** est déclenchée si les tentatives continuent à 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 volume effectuées avec succès.



Les tailles ne s'appliquent pas aux objets répliqués et apparaissent uniquement pour les restaurations contenant des objets de données avec code d'effacement (EC).

Vérifier l'état du stockage après la récupération d'un nœud de stockage StorageGRID

Après avoir restauré 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 est **En ligne** par défaut à chaque redémarrage du serveur de nœud de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **Nœuds** > **Nœud de stockage** > **Tâches**.
2. Si la liste déroulante **État de stockage** est définie sur **Lecture seule** ou **Hors ligne**, sélectionnez **En ligne**.
3. Sélectionnez **Enregistrer**.

Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact

Avertissements concernant la récupération des volumes de stockage StorageGRID

Avant de restaurer 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 des bases de données Cassandra, tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres volumes de stockage sont utilisés exclusivement pour les données d'objet.

La base de données Cassandra peut être reconstruite dans le cadre de la procédure de récupération du volume si :

- Le volume 0 échoue et est récupéré.
- Le lecteur système et un ou plusieurs volumes de stockage sont défectueux et restaurés.

Lorsque Cassandra est reconstruit, le système utilise les informations provenant d'autres nœuds de stockage. Si Cassandra a été reconstruit récemment, les données Cassandra peuvent ne pas encore être cohérentes sur l'ensemble de la grille. Si trop de nœuds de stockage sont hors ligne :

- Certaines données Cassandra peuvent ne pas être disponibles.
- Une perte de données pourrait survenir.



Si plusieurs nœuds de stockage sont en panne (ou sont hors ligne), contactez le support technique. N'exécutez pas la procédure de récupération suivante. Une perte de données pourrait survenir. Pour plus d'informations, reportez-vous à ["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 associées

["Avertissements et considérations relatives à la restauration des nœuds de la grille"](#)

Identifier et démonter les volumes de stockage défaillants dans StorageGRID

Lors de la restauration d'un nœud de stockage dont les volumes de stockage sont en panne, vous devez identifier et démonter les volumes en panne. Vous devez vérifier que seuls les volumes de stockage défaillants sont reformatés dans le cadre de la procédure de restauration.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).

Description de la tâche

Vous devriez récupérer les volumes de stockage défaillants dès que possible.

La première étape du processus de restauration consiste à détecter les volumes qui se sont détachés, qui doivent être démontés ou qui présentent des erreurs d'E/S. Si les volumes défaillants sont toujours attachés mais qu'un système de fichiers est corrompu de façon aléatoire, le système risque de ne pas détecter de corruption dans les pièces non utilisées ou non attribuées du disque.



Vous devez terminer cette procédure avant d'effectuer manuellement les étapes de restauration des volumes, telles que l'ajout ou la reconfiguration des disques, l'arrêt du nœud, le démarrage du nœud ou le redémarrage. Sinon, lorsque vous exécutez `reformat_storage_block_devices.rb` le script, vous risquez de rencontrer une erreur du système de fichiers qui provoque le blocage ou l'échec du script.



Réparez le matériel et connectez correctement les disques avant d'exécuter `reboot` la commande.



Identifiez minutieusement les volumes de stockage défaillants. Ces informations vous permettront de vérifier quels volumes doivent être reformatés. Une fois qu'un volume a été reformaté, les données du volume ne peuvent pas être récupérées.

Pour récupérer 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 point de montage, le nom du périphérique et la taille du volume sont affichés dans le gestionnaire de grille.

Étapes

1. Procédez comme suit pour enregistrer les volumes de stockage défaillants et leurs noms de périphériques :
 - a. Sélectionnez **Nœuds > site > nœud de stockage défaillant > Stockage**.
 - b. Faites défiler vers le bas pour localiser la table Volumes et la table Magasins d'objets et enregistrez les informations suivantes pour chaque volume avec un statut Inconnu ou Hors ligne.
 - Dans la table Volumes, enregistrez le point de montage, le périphérique et la taille.
 - À partir de la table des magasins d'objets, enregistrez le `object_store_ID`.

Le `object_store_ID` correspond à l'ID du volume de stockage défaillant. Par exemple, spécifiez 0 dans la commande d'un magasin d'objets ayant l'ID 0000.

2. Connectez-vous au nœud de stockage défaillant :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. Exécutez le script suivant pour démonter un volume de stockage défaillant :

```
sn-unmount-volume object_store_ID
```

4. Si vous y êtes invité, appuyez sur **y** pour arrêter le service Cassandra en fonction du volume de stockage 0.



Si le service Cassandra est déjà arrêté, vous n'êtes pas invité à le faire. Le service Cassandra est arrêté uniquement pour le volume 0.

```

root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.

```

Le volume est démonté en quelques secondes. Des messages s'affichent indiquant chaque étape du processus. Le dernier message indique que le volume est démonté.

5. Si le démontage échoue parce que le volume est occupé, vous pouvez forcer le démontage à l'aide de l'option `--use-umountof` :



Forcer un démontage à l'aide de l'option peut provoquer un comportement inattendu ou un `--use-umountof` blocage des processus ou services utilisant le volume.

```

root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes

```

Récupérez les volumes de stockage défaillants et reconstruisez la base de données Cassandra dans StorageGRID

Vous devez exécuter un script qui reformate et remonte le stockage sur les volumes de stockage défaillants, puis reconstitue la base de données Cassandra sur le nœud de stockage si le système détermine qu'elle est nécessaire.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.
- Les lecteurs système du serveur sont intacts.
- La cause de la défaillance a été identifiée et, si nécessaire, le matériel de stockage de remplacement a déjà été acquis.
- La taille totale du stockage de remplacement est la même que celle de l'original.
- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou 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.**)
- Vous avez ["vérifié les avertissements concernant la restauration du volume de stockage"](#).

Étapes

1. Si nécessaire, remplacez le stockage physique ou virtuel défectueux associé aux volumes de stockage défectueux que vous avez identifiés et démontés précédemment.

Ne remontez pas les volumes lors de cette étape. Le stockage est remonté et ajouté à `/etc/fstab` dans une étape ultérieure.

2. Dans le gestionnaire de grille, accédez à **Nœuds > 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

4. Utilisez un éditeur de texte (vi ou vim) pour supprimer les volumes en échec du `/etc/fstab` fichier, puis enregistrez le fichier.



Le commentaire d'un volume en échec dans le `/etc/fstab` fichier est insuffisant. Le volume doit être supprimé de `fstab` car le processus de restauration vérifie que toutes les lignes du `fstab` fichier correspondent aux systèmes de fichiers montés.

5. Reformatez 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.
 - Si nécessaire, vous serez invité à reconstruire la base de données Cassandra.
 - Examinez les avertissements. Si aucune d'entre elles ne s'applique, reconstruisez la base de données Cassandra. Saisissez : **y**
 - Si plusieurs nœuds de stockage sont hors ligne. Entrez : **n**

Le script s'quitte sans reconstruire Cassandra. Contactez l'assistance technique.

- Pour chaque lecteur `rangedb` sur le nœud de stockage, lorsque vous êtes invité à : `Reformat the rangedb drive <name> (device <major number>:<minor number>) ? [y/n]?`, entrez l'une des réponses suivantes :
 - **y** pour reformater un lecteur qui a eu des erreurs. Ceci reformate le volume de stockage et ajoute le volume de stockage reformaté au `/etc/fstab` fichier.
 - **n** si le lecteur ne contient aucune erreur et que vous ne voulez pas le reformater.



La sélection de **n** ferme le script. Montez le lecteur (si vous pensez que les données du lecteur doivent être conservées et que le lecteur a été démonté par erreur) ou retirez le lecteur. Ensuite, exécutez de nouveau la `reformat_storage_block_devices.rb` commande.



Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être une sortie de script mentionnant « Reaper » ou « Cassandra repair ». Si un message d'erreur s'affiche, 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 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.
```

Et ensuite ?

Une fois les volumes de stockage reformatés et remontés et les opérations Cassandra nécessaires terminées, vous pouvez ["Restaurez les données d'objet à l'aide de Grid Manager"](#).

Restaurez les données d'objet sur le volume de stockage StorageGRID où le lecteur système est intact

Après avoir restauré un volume de stockage sur un nœud de stockage sur lequel le disque système est intact, vous pouvez restaurer les données d'objet répliquées ou avec code d'effacement qui ont été perdues en cas de défaillance du volume de stockage.

Avant de commencer

- Si la procédure automatique n'a pas permis de remonter les volumes de stockage préservés et de reformatier les volumes de stockage défectueux, vous avez effectué l'une des procédures suivantes :
 - ["Remontage et reformatage des volumes de stockage de l'appliance \(étapes manuelles\)"](#)
 - ["Remontage et reformatage des volumes de stockage \(étapes manuelles\)"](#)
- Vous avez confirmé que le nœud de stockage sur lequel vous restaurez des objets a un état de connexion **Connecté**  sur l'onglet **Nœuds** > **Vue d'ensemble** dans le Grid Manager.
- Vous avez confirmé ce qui suit :

- L'extension de la grille pour ajouter un nœud de stockage n'est pas en cours.
- La mise hors service d'un nœud de stockage n'est pas en cours ni échouée.
- La récupération d'un volume de stockage défaillant n'est pas en cours.
- La récupération d'un nœud de stockage dont le disque système est défaillant n'est pas en cours.
- Aucune opération de rééquilibrage de l'EC n'est en cours.
- Le clonage des nœuds d'appliance n'est pas en cours.

Description de la tâche

Une fois les disques remplacés et les volumes formatés, Grid Manager affiche les volumes comme candidats à la restauration dans l'onglet **Maintenance > Restauration de volume > Nœuds à restaurer**.

Lorsque cela est possible, restaurez les données d'objet à l'aide de la page Restauration des volumes du Gestionnaire de grille. Vous pouvez soit [activer le mode de restauration automatique](#) lancer automatiquement la restauration du volume lorsque les volumes sont prêts à être restaurés, soit [effectuez manuellement la restauration des volumes](#). Suivez ces instructions :

- 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 sont en panne, mais pas tous
 - Tous les volumes de stockage d'un nœud sont en panne et sont remplacés par le même nombre de volumes ou plus

La page de restauration de volume dans le gestionnaire de grille vous permet également de [surveiller le processus de restauration des volumes](#) et [afficher l'historique de restauration](#).

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, contactez le support technique pour obtenir de l'aide.

Vous pouvez restaurer deux types de données d'objet :

- Les objets de données répliqués sont restaurés à partir d'autres emplacements, dans la mesure où les règles ILM de la grille ont été configurées de façon à rendre disponibles les copies objet.
 - Si une règle ILM a été configurée pour ne stocker qu'une seule copie répliquée et que cette copie se trouvait 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 demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet.
- Les objets de données avec code d'effacement (EC) sont restaurés en réassemblez les fragments stockés. Les fragments corrompus ou perdus sont recréés par l'algorithme de code d'effacement à partir des fragments de données et de parité restants.

Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.



La restauration des volumes dépend de la disponibilité des ressources dans lesquelles les copies objet sont stockées. La progression de la restauration des volumes n'est pas linéaire et peut prendre des jours ou des semaines.

Active le mode de restauration automatique

Lorsque vous activez le mode de restauration automatique, la restauration des volumes 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 activé.
3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails.



- Vous ne pourrez pas lancer manuellement de tâches de restauration de volume sur aucun nœud.
- Les restaurations de volume ne démarrent automatiquement que lorsqu'aucune autre procédure de maintenance n'est en cours.
- Vous pouvez contrôler l'état du travail à partir de la page de surveillance de la progression.
- StorageGRID relance automatiquement les restaurations de volume qui ne démarrent pas.

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.

[[restauration manuelle]] restaurez manuellement un volume ou un nœud défaillant

Procédez comme suit 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 de **mode de restauration automatique** sur la position Désactivé.

Le numéro de l'onglet indique le nombre de nœuds pour lesquels des volumes nécessitent une restauration.

3. Développez chaque nœud pour afficher les volumes qui nécessitent une restauration, ainsi que leur état.
4. Corrigez tous les problèmes empêchant la restauration de chaque volume. Les problèmes sont indiqués lorsque vous sélectionnez **en attente d'étapes manuelles**, s'il s'affiche comme état du volume.
5. Sélectionnez un nœud à restaurer où tous les volumes indiquent l'état prêt pour la restauration.

Vous ne pouvez restaurer les volumes que pour un nœud à la fois.

Chaque volume du nœud doit indiquer qu'il est prêt à être restauré.

6. Sélectionnez **Démarrer la restauration**.

7. Réglez les avertissements qui peuvent apparaître ou sélectionnez **Démarrer malgré tout** pour ignorer les avertissements et lancer la restauration.

Les nœuds sont déplacés de l'onglet **nœuds à restaurer** vers l'onglet **progression de la restauration** au démarrage de la restauration.

Si une restauration de volume ne peut pas être démarrée, le nœud revient à l'onglet **nœuds à restaurer**.

Afficher la progression de la restauration

L'onglet **progression de la restauration** affiche l'état du processus de restauration du volume et des informations sur les volumes d'un nœud restauré.

Les taux de réparation des données pour les objets répliqués et ceux dont le codage d'effacement est utilisé dans tous les volumes correspondent à des moyennes résumant toutes les restaurations en cours. Le pourcentage d'objets dans ces volumes qui sont intacts et ne nécessitent aucune restauration est également indiqué.



La restauration des données répliquées dépend de la disponibilité des ressources dans lesquelles les copies répliquées sont stockées. La progression de la restauration des données répliquées n'est pas linéaire et peut prendre des jours ou des semaines.

La section tâches de restauration affiche des informations sur les restaurations de volume démarrées à partir du Gestionnaire de grille.

- Le nombre indiqué dans l'en-tête de la section travaux de restauration indique le nombre de volumes en cours de restauration ou en file d'attente de restauration.
- Le tableau affiche des informations sur chaque volume d'un nœud en cours de restauration ainsi que sa progression.
 - La progression de chaque nœud affiche le pourcentage pour chaque travail.
 - Développez la colonne Détails pour afficher l'heure de début de la restauration et l'ID du travail.
- En cas d'échec de la restauration d'un volume :
 - La colonne État indique `failed (attempting retry)`, et sera réexécutée automatiquement.
 - Si plusieurs travaux de restauration ont échoué, le travail le plus récent sera automatiquement repassé en premier.
 - L'alerte **EC repair failure** est déclenchée si les tentatives continuent à 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 volume effectuées avec succès.



Les tailles ne s'appliquent pas aux objets répliqués et apparaissent uniquement pour les restaurations contenant des objets de données avec code d'effacement (EC).

Vérifiez l'état du stockage après la récupération des volumes de stockage StorageGRID

Après la récupération des 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 Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **Nœuds** > **Nœud de stockage** > **Tâches**.
2. Si la liste déroulante **État de stockage** est définie sur Lecture seule ou Hors ligne, sélectionnez **En ligne**.
3. Sélectionnez **Enregistrer**.

Restaurez les données après une panne de disque système

Avertissements pour la récupération du disque système du nœud de stockage StorageGRID

Avant de restaurer un lecteur système défaillant d'un nœud de stockage, consultez les avertissements généraux ["avertissements et remarques concernant la restauration d'un nœud grid"](#) et 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 si :

- Un volume de stockage tombe en panne et est récupéré.
- Le lecteur système et un ou plusieurs volumes de stockage sont défectueux et restaurés.

Lorsque Cassandra est reconstruit, le système utilise les informations provenant d'autres nœuds de stockage. Si Cassandra a été reconstruit récemment, les données Cassandra peuvent ne pas encore être cohérentes sur l'ensemble de la grille. Si trop de nœuds de stockage sont hors ligne :

- Certaines données Cassandra peuvent ne pas être disponibles.
- Une perte de données pourrait survenir.



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. Pour plus d'informations, reportez-vous à ["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 dont les volumes de stockage sont défaillants, récupérez les volumes sur le nœud de stockage dont les volumes de stockage sont défaillants avant de récupérer ce nœud de stockage défaillant. Consultez les instructions pour ["effectuez des restaurations après une panne du volume de stockage, là où le disque système est intact"](#).



Si les règles ILM sont configurées pour ne stocker qu'une seule copie répliquée, et si cette copie existe sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.

Remplacer le nœud de stockage StorageGRID

Si le lecteur du système est défectueux, vous devez d'abord remplacer le nœud de stockage.

Vous devez sélectionner la procédure de remplacement de nœuds pour votre plate-forme. Les étapes à suivre pour remplacer un nœud sont les mêmes pour tous les types de nœuds de la grille.



Cette procédure s'applique uniquement aux nœuds de stockage basés sur logiciel. Vous devez suivre une procédure différente de ["Restaurer un nœud de stockage d'appliance"](#).

Linux: si vous n'êtes pas sûr que votre lecteur système est en panne, suivez les instructions pour remplacer le nœud afin de déterminer les étapes de récupération requises.

Plateforme	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Ensuite, suivez la procédure pour "Remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud de stockage StorageGRID

Après avoir remplacé un noeud de stockage, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.
- Vous disposez de la date de début des travaux de réparation pour les données avec code d'effacement.

Description de la tâche

Si le nœud de stockage est installé en tant que conteneur sur un hôte Linux, vous devez effectuer cette étape uniquement si l'un d'entre eux est vrai :

- Vous deviez utiliser l'`--force``indicateur pour importer le nœud, ou vous avez émis ``storagegrid node force-recovery node-name`

- Vous deviez réinstaller un nœud complet ou restaurer /var/local.

Étapes

1. Connectez-vous au nœud d'administration principal. Si le nœud d'administration principal est indisponible, utilisez un nœud d'administration non principal, s'il en existe un.
2. Dans le Grid Manager, sélectionnez **Maintenance > Tasks > Node recovery**.
3. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

4. Saisissez la **phrase secrète de provisionnement**.
5. Cliquez sur **Démarrer la récupération**.
6. Surveillez la progression de la récupération en sélectionnant **Maintenance > Tasks > Node recovery** et en consultant la progression de la récupération.
 - Si le nœud de la grille atteint l'étape « En attente d'instructions manuelles », vous devez ["Remontez et reformatez manuellement les volumes de stockage"](#). Une fois les instructions manuelles terminées, passez à ["restaurer les données d'objet sur les volumes"](#).
 - Si la récupération du nœud de grid est passée de **En cours** à **Récupéré** sans passer par l'étape « Waiting for manual steps », aucune autre action n'est requise.



À tout moment pendant la récupération, vous pouvez sélectionner **Réinitialiser** pour lancer une nouvelle récupération. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.

Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appliance à son état préinstallé, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux :

```
storagegrid node force-recovery node-name
```

Remonter et reformater les volumes de stockage StorageGRID (étapes manuelles)

Si la procédure automatique ne parvient pas à remonter les volumes de stockage préservés et à reformater les volumes de stockage défaillants, vous devez exécuter manuellement deux scripts pour effectuer ces opérations. Le premier script remonte les volumes correctement formatés en tant que volumes de stockage StorageGRID. Le second script reformate les volumes non montés, reconstruit la base de données Cassandra si nécessaire et démarre les services.

Lors de la récupération d'un nœud de stockage, si le message « En attente d'instructions manuelles » s'affiche dans le Gestionnaire de grille, suivez ces étapes pour remonter et reformater les volumes de stockage. Si ce message ne s'affiche pas, les opérations de remontage et de reformatage se sont terminées automatiquement, et vous pouvez ignorer *cette* procédure et ["restaurer les données de l'objet"](#).

Avant de commencer

- Vous avez déjà remplacé le matériel de tous les volumes de stockage défectueux que vous savez avoir besoin d'être remplacé.

L'exécution `sn-remount-volumes` du script peut vous aider à identifier d'autres volumes de stockage 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.**)
- Vous avez "[Consultez les avertissements relatifs à la restauration du lecteur du système du nœud de stockage](#)".



Contactez le support technique si plusieurs nœuds de stockage sont hors ligne. Ne courez pas le `sn-recovery-postinstall.sh` scénario.

Description de la tâche

Pour effectuer cette procédure, vous devez effectuer les tâches de haut niveau suivantes :

- Connectez-vous au nœud de stockage récupéré.
- Exécutez `sn-remount-volumes` le script pour remonter les volumes de stockage correctement formatés. Lorsque ce script s'exécute, il effectue les opérations suivantes :
 - Monte et démonte chaque volume de stockage pour relire le journal XFS.
 - Effectue une vérification de cohérence de fichier XFS.
 - Si le système de fichiers est cohérent, détermine si le volume de stockage est un volume de stockage StorageGRID correctement formaté.
 - Si le volume de stockage est correctement formaté, remonter le volume de stockage. Toutes les données existantes du volume restent intactes.
- Examinez la sortie du script et résolvez tout problème.
- Exécutez `sn-recovery-postinstall.sh` le script. Lorsque ce script s'exécute, il effectue les opérations suivantes :



Ne redémarrez pas un nœud de stockage pendant la restauration avant de l'exécuter `sn-recovery-postinstall.sh` pour reformater les volumes de stockage défaillants et restaurer les métadonnées de l'objet. Le redémarrage du nœud de stockage avant la `sn-recovery-postinstall.sh` fin de entraîne des erreurs pour les services qui tentent de démarrer et provoque la sortie du mode de maintenance par les nœuds d'appliance StorageGRID. Voir l'étape pour [script post-installation](#).

- Reformate les volumes de stockage que le script n'a pas pu monter ou dont le `sn-remount-volumes` formatage a été incorrect.



Lorsqu'un volume de stockage est reformaté, toutes les données de ce volume sont perdues. Vous devez effectuer une procédure supplémentaire pour restaurer les données d'objet à partir d'autres emplacements de la grille, en supposant que les règles ILM ont été configurées pour stocker plusieurs copies d'objet.

- 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`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Exécutez le premier script pour remonter tous les volumes de stockage correctement formatés.



Si tous les volumes de stockage sont nouveaux et doivent être formatés, ou si tous les volumes de stockage ont échoué, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage démontés.

- Exécutez le script : `sn-remount-volumes`

Ce script peut prendre des heures sur les volumes de stockage qui contiennent des données.

- Au fur et à mesure de l'exécution du script, vérifiez le résultat et répondez aux invites.



Si nécessaire, vous pouvez utiliser `tail -f` la commande pour contrôler le contenu du fichier journal du script (`/var/local/log/sn-remount-volumes.log`) . Le fichier journal contient des informations plus détaillées que la sortie de la ligne de commande.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
```

You can see the diagnosis information in the `/var/local/log/sn-remount-volumes.log`.

This volume could be new or damaged. If you run `sn-recovery-postinstall.sh`, this volume and any data on this volume will be deleted. If you only had two copies of object data, you will temporarily have only a single copy. StorageGRID 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 ont rencontré des erreurs.

- /dev/sdb La vérification de la cohérence du système de fichiers XFS a été effectuée et la structure de volume était valide. Le montage a donc réussi. Les données sur les périphériques 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 impossible de monter car le disque n'a pas été initialisé ou le superbloc du disque a été corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter le contrôle de cohérence du système de fichiers.
 - Si le volume de stockage est relié à un nouveau disque, répondez **N** à l'invite. Vous n'avez pas besoin de vérifier le système de fichiers sur un nouveau disque.
 - Si le volume de stockage est relié à un disque existant, répondez **y** à l'invite. Vous pouvez utiliser les résultats de la vérification du système de fichiers pour déterminer la source de la corruption. Les résultats sont enregistrés dans le /var/local/log/sn-remount-volumes.log fichier journal.
- /dev/sde Le contrôle de cohérence du système de fichiers XFS a été effectué et la structure de volume était valide. Cependant, l'ID de nœud LDR dans le fichier volID ne correspond pas à l'ID de ce nœud de stockage (`configured LDR noid`affiché en haut). Ce message indique que ce volume appartient à un autre nœud de stockage.

3. Examinez la sortie du script et résolvez tout problème.



Si un volume de stockage a échoué au contrôle de cohérence du système de fichiers XFS ou ne peut pas être monté, vérifiez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution `sn-recovery-postinstall.sh` du script sur ces volumes.

- a. Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si aucun volume n'est répertorié, exécutez à nouveau le script.
- b. Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a pas d'erreur indiquant qu'un volume de stockage n'appartient pas à ce nœud de stockage.

Dans l'exemple, la sortie de `/dev/sde` inclut le message d'erreur suivant :

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Si un volume de stockage est signalé comme appartenant à un autre nœud de stockage, contactez le support technique. Si vous exécutez `sn-recovery-postinstall.sh` le script, le volume de stockage sera reformaté, ce qui pourrait entraîner une perte de données.

- c. Si aucun périphérique de stockage n'a pu être monté, notez le nom du périphérique et réparez ou remplacez le périphérique.



Vous devez réparer ou remplacer tout périphérique de stockage qui n'a pas pu être monté.

- d. Après avoir réparé ou remplacé tous les périphériques unmountable, exécutez à nouveau le `sn-remount-volumes` script pour confirmer que tous les volumes de stockage pouvant être remontés ont été remontés.



Si un volume de stockage ne peut pas être monté ou est mal formaté et que vous passez à l'étape suivante, le volume et toutes les données du volume seront supprimés. Si vous aviez deux copies de vos données d'objet, vous n'aurez qu'une seule copie jusqu'à la fin de la procédure suivante (restauration des données d'objet).



N'exécutez pas `sn-recovery-postinstall.sh` le script si vous pensez que les données restantes sur un volume de stockage défaillant ne peuvent pas être reconstruites à partir d'un autre emplacement de la grille (par exemple, si votre règle 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 savoir comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` script : `sn-recovery-postinstall.sh`

Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui n'ont pas été correctement formatés. Reconstitue la base de données Cassandra sur le nœud, si nécessaire, et démarre les services sur le nœud de stockage.

Gardez à l'esprit les points suivants :

- L'exécution du script peut prendre des heures.
- En général, vous devez laisser la session SSH seule pendant que le script est en cours d'exécution.
- N'appuyez pas sur **Ctrl+C** lorsque la session SSH est active.
- Le script s'exécute en arrière-plan en cas d'interruption du réseau et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page récupération.
- Si le nœud de stockage utilise le service RSM, le script peut sembler bloqué pendant 5 minutes au redémarrage des services de nœud. Ce délai de 5 minutes est prévu lorsque l'entretien du RSM démarre pour la première fois.



Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.



Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être une sortie de script mentionnant « Reaper » ou « Cassandra repair ». Si un message d'erreur s'affiche, indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

5. au fur et à mesure de `sn-recovery-postinstall.sh` l'exécution du script, surveillez la page récupération dans le Gestionnaire de grille.

La barre de progression et la colonne Stage de la page récupération fournissent un état de haut niveau du `sn-recovery-postinstall.sh` script.

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 Q				
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. Une fois que le `sn-recovery-postinstall.sh` script a démarré les services sur le nœud, vous pouvez restaurer les données d'objet sur tous les volumes de stockage formatés par le script.

Le script vous demande si vous souhaitez utiliser le processus de restauration du volume Grid Manager.

- Dans la plupart des cas, vous devriez "[Restaurez les données d'objet à l'aide de Grid Manager](#)". Répondez `y` pour utiliser le Gestionnaire de grille.
- Dans de rares cas, par exemple si le nœud de remplacement dispose de moins de volumes disponibles pour le stockage d'objets que le nœud d'origine, contactez le support technique pour restaurer manuellement les données d'objets. Si l'un de ces cas s'applique, répondez `n` et appuyez sur

n'importe quelle touche pour revenir à la ligne de commandes.

Restaurer les données d'objet sur le volume de stockage StorageGRID (panne disque)

Après avoir restauré des volumes de stockage sur un nœud de stockage non appliance, vous pouvez restaurer les données d'objet répliquées ou codées en effacement qui ont été perdues en cas de défaillance du nœud de stockage.

Avant de commencer

- Si la procédure automatique n'a pas permis de remonter les volumes de stockage préservés et de reformatier les volumes de stockage défaillants, vous avez effectué l'une des procédures suivantes :
 - ["Remontage et reformatage des volumes de stockage de l'appliance \(étapes manuelles\)"](#)
 - ["Remontage et reformatage des volumes de stockage \(étapes manuelles\)"](#)
- Vous avez confirmé que le nœud de stockage sur lequel vous restaurez des objets a un état de connexion **Connecté**  sur l'onglet **Nœuds** > **Vue d'ensemble** dans le Grid Manager.
- Vous avez confirmé ce qui suit :
 - L'extension de la grille pour ajouter un nœud de stockage n'est pas en cours.
 - La mise hors service d'un nœud de stockage n'est pas en cours ni échouée.
 - La récupération d'un volume de stockage défaillant n'est pas en cours.
 - La récupération d'un nœud de stockage dont le disque système est défaillant n'est pas en cours.
 - Aucune opération de rééquilibrage de l'EC n'est en cours.
 - Le clonage des nœuds d'appliance n'est pas en cours.

Description de la tâche

Une fois les disques remplacés et les volumes formatés, Grid Manager affiche les volumes comme candidats à la restauration dans l'onglet **Maintenance** > **Restauration de volume** > **Nœuds à restaurer**.

Lorsque cela est possible, restaurez les données d'objet à l'aide de la page Restauration des volumes du Gestionnaire de grille. Vous pouvez soit [activer le mode de restauration automatique](#) lancer automatiquement la restauration du volume lorsque les volumes sont prêts à être restaurés, soit [effectuez manuellement la restauration des volumes](#). Suivez ces instructions :

- 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 sont en panne, mais pas tous
 - Tous les volumes de stockage d'un nœud sont en panne et sont remplacés par le même nombre de volumes ou plus

La page de restauration de volume dans le gestionnaire de grille vous permet également de [surveiller le processus de restauration des volumes](#) et [afficher l'historique de restauration](#).

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, contactez le support technique pour obtenir de l'aide.

Vous pouvez restaurer deux types de données d'objet :

- Les objets de données répliqués sont restaurés à partir d'autres emplacements, dans la mesure où les règles ILM de la grille ont été configurées de façon à rendre disponibles les copies objet.
 - Si une règle ILM a été configurée pour ne stocker qu'une seule copie répliquée et que cette copie se trouvait 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 demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet.
- Les objets de données avec code d'effacement (EC) sont restaurés en réassemblez les fragments stockés. Les fragments corrompus ou perdus sont recréés par l'algorithme de code d'effacement à partir des fragments de données et de parité restants.

Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.



La restauration des volumes dépend de la disponibilité des ressources dans lesquelles les copies objet sont stockées. La progression de la restauration des volumes n'est pas linéaire et peut prendre des jours ou des semaines.

Active le mode de restauration automatique

Lorsque vous activez le mode de restauration automatique, la restauration des volumes 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 activé.
3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails.



- Vous ne pourrez pas lancer manuellement de tâches de restauration de volume sur aucun nœud.
- Les restaurations de volume ne démarrent automatiquement que lorsqu'aucune autre procédure de maintenance n'est en cours.
- Vous pouvez contrôler l'état du travail à partir de la page de surveillance de la progression.
- StorageGRID relance automatiquement les restaurations de volume qui ne démarrent pas.

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.

[[restauration manuelle]] restaurez manuellement un volume ou un nœud défaillant

Procédez comme suit 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 de **mode de restauration automatique** sur la position Désactivé.

Le numéro de l'onglet indique le nombre de nœuds pour lesquels des volumes nécessitent une restauration.

3. Développez chaque nœud pour afficher les volumes qui nécessitent une restauration, ainsi que leur état.
4. Corrigez tous les problèmes empêchant la restauration de chaque volume. Les problèmes sont indiqués lorsque vous sélectionnez **en attente d'étapes manuelles**, s'il s'affiche comme état du volume.
5. Sélectionnez un nœud à restaurer où tous les volumes indiquent l'état prêt pour la restauration.

Vous ne pouvez restaurer les volumes que pour un nœud à la fois.

Chaque volume du nœud doit indiquer qu'il est prêt à être restauré.

6. Sélectionnez **Démarrer la restauration**.
7. Réglez les avertissements qui peuvent apparaître ou sélectionnez **Démarrer malgré tout** pour ignorer les avertissements et lancer la restauration.

Les nœuds sont déplacés de l'onglet **nœuds à restaurer** vers l'onglet **progression de la restauration** au démarrage de la restauration.

Si une restauration de volume ne peut pas être démarrée, le nœud revient à l'onglet **nœuds à restaurer**.

Afficher la progression de la restauration

L'onglet **progression de la restauration** affiche l'état du processus de restauration du volume et des informations sur les volumes d'un nœud restauré.

Les taux de réparation des données pour les objets répliqués et ceux dont le codage d'effacement est utilisé dans tous les volumes correspondent à des moyennes résumant toutes les restaurations en cours. Le pourcentage d'objets dans ces volumes qui sont intacts et ne nécessitent aucune restauration est également indiqué.



La restauration des données répliquées dépend de la disponibilité des ressources dans lesquelles les copies répliquées sont stockées. La progression de la restauration des données répliquées n'est pas linéaire et peut prendre des jours ou des semaines.

La section tâches de restauration affiche des informations sur les restaurations de volume démarrées à partir du Gestionnaire de grille.

- Le nombre indiqué dans l'en-tête de la section travaux de restauration indique le nombre de volumes en cours de restauration ou en file d'attente de restauration.
- Le tableau affiche des informations sur chaque volume d'un nœud en cours de restauration ainsi que sa progression.
 - La progression de chaque nœud affiche le pourcentage pour chaque travail.
 - Développez la colonne Détails pour afficher l'heure de début de la restauration et l'ID du travail.
- En cas d'échec de la restauration d'un volume :

- La colonne **État** indique `failed (attempting retry)`, et sera réexécutée automatiquement.
- Si plusieurs travaux de restauration ont échoué, le travail le plus récent sera automatiquement repassé en premier.
- L'alerte **EC repair failure** est déclenchée si les tentatives continuent à 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 volume effectuées avec succès.



Les tailles ne s'appliquent pas aux objets répliqués et apparaissent uniquement pour les restaurations contenant des objets de données avec code d'effacement (EC).

Vérifiez l'état du stockage après la récupération d'un disque système StorageGRID Storage Node

Après avoir restauré 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 est en ligne par défaut à chaque redémarrage du serveur de nœud de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **Nœuds** > **Nœud de stockage** > **Tâches**.
2. Si la liste déroulante **État de stockage** est définie sur **Lecture seule** ou **Hors ligne**, sélectionnez **En ligne**.
3. Sélectionnez **Enregistrer**.

Restaurez vos données après une panne de nœud d'administration

Récupération du nœud d'administration principal ou non principal dans StorageGRID

Le processus de restauration d'un nœud d'administration dépend du nœud d'administration principal ou non primaire.

Les étapes générales de restauration d'un nœud d'administration principal ou non primaire sont les mêmes, bien que les détails de la procédure diffèrent.

Suivez toujours la procédure de récupération correcte pour le nœud d'administration que vous restaurez. Les procédures semblent identiques à un niveau élevé, mais diffèrent dans les détails.

Choix

- ["Récupérez le nœud d'administration principal en utilisant le même nœud d'administration principal"](#)
- ["Récupérez après des défaillances du nœud d'administration principal à l'aide d'un nœud d'administration non principal"](#)

- ["Restaurez vos données en cas de défaillance d'un nœud d'administration non principal"](#)

Récupérez après une défaillance du nœud d'administration principal en utilisant le même nœud d'administration principal

Récupérez le nœud d'administration principal StorageGRID en utilisant le même nœud d'administration principal.

Vous devez effectuer un ensemble spécifique de tâches pour effectuer une restauration suite à une défaillance d'un nœud d'administration principal. Le nœud d'administration principal héberge le service de nœud de gestion de la configuration (CMN) pour la grille.



Vous devez réparer ou remplacer rapidement un nœud d'administration principal défaillant, faute de quoi vous risquez de ne pas pouvoir effectuer certaines opérations de maintenance.

Pour restaurer un nœud d'administration principal, suivez ces étapes générales :

1. ["La copie des journaux d'audit à partir d'un nœud d'administration principal a échoué"](#)
2. ["Remplacez le nœud d'administration principal"](#)
3. ["Configurez le nœud d'administration principal de remplacement"](#)
4. ["Déterminez si un correctif est requis pour le nœud d'administration principal récupéré"](#)
5. ["Restaurez le journal d'audit sur le nœud d'administration principal restauré"](#)
6. ["Restaurez la base de données du nœud d'administration lors de la récupération d'un nœud d'administration principal"](#)
7. ["Restauration de metrics Prometheus lors de la restauration d'un nœud d'administration principal"](#)

Copier les journaux d'audit à partir d'un nœud d'administration principal StorageGRID défaillant

Si vous pouvez copier les journaux d'audit à partir du nœud d'administration principal défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration principal restauré une fois qu'il est en cours d'exécution.

Description de la tâche

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.



Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

Étapes

1. Connectez-vous au nœud d'administration principal défaillant, si possible. Sinon, connectez-vous à n'importe quel nœud d'administration disponible.
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal : `service ams stop`
3. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/audit/export
```

(ou `cd /var/local/log` sur les systèmes antérieurs)

4. Renommez le fichier journal source avec un nom de fichier numéroté unique.



- Si le fichier journal est dans le `/var/local/audit/export` répertoire, son nom est `audit.log`.
- Si le fichier journal est dans le `/var/local/log` répertoire, son nom est `localaudit.log`.

Par exemple, renommez le `localaudit.log` fichier à `2025-10-22.txt.1`.

```
ls -l  
mv localaudit.log 2025-10-22.txt.1
```

5. Redémarrez le service AMS : `service ams start`
6. Créez le répertoire pour copier tous les fichiers journaux d'audit dans un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

7. Copiez tous les fichiers journaux d'audit à l'emplacement temporaire : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

8. Se déconnecter en tant que root : `exit`

Remplacez le nœud d'administration principal StorageGRID en utilisant le même nœud d'administration principal

Pour restaurer un nœud d'administration principal, vous devez d'abord remplacer le matériel physique ou virtuel.

Pour restaurer 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 fonctionnant sur la même plateforme.
- Vous pouvez remplacer un nœud d'administration principal exécuté sur VMware ou un hôte Linux par un nœud d'administration principal hébergé sur une appliance de services StorageGRID.
- Vous pouvez remplacer un nœud d'administration principal exécuté sur un hôte VMware par un appliance de services SG1000 ou SG100.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement des nœuds (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration du nœud d'administration principal.

Et de remplacement	Procédure
VMware	"Remplacer un nœud VMware par un nœud de récupération" "Remplacez un nœud VMware par un SG1000 ou un SG100"
Linux	"Remplacer un nœud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Ensuite, suivez la procédure pour "Remplacement d'un nœud Linux" .

Configurez un nœud d'administration principal de remplacement dans StorageGRID

Le nœud de remplacement doit être configuré en tant que nœud d'administration principal de votre système StorageGRID.

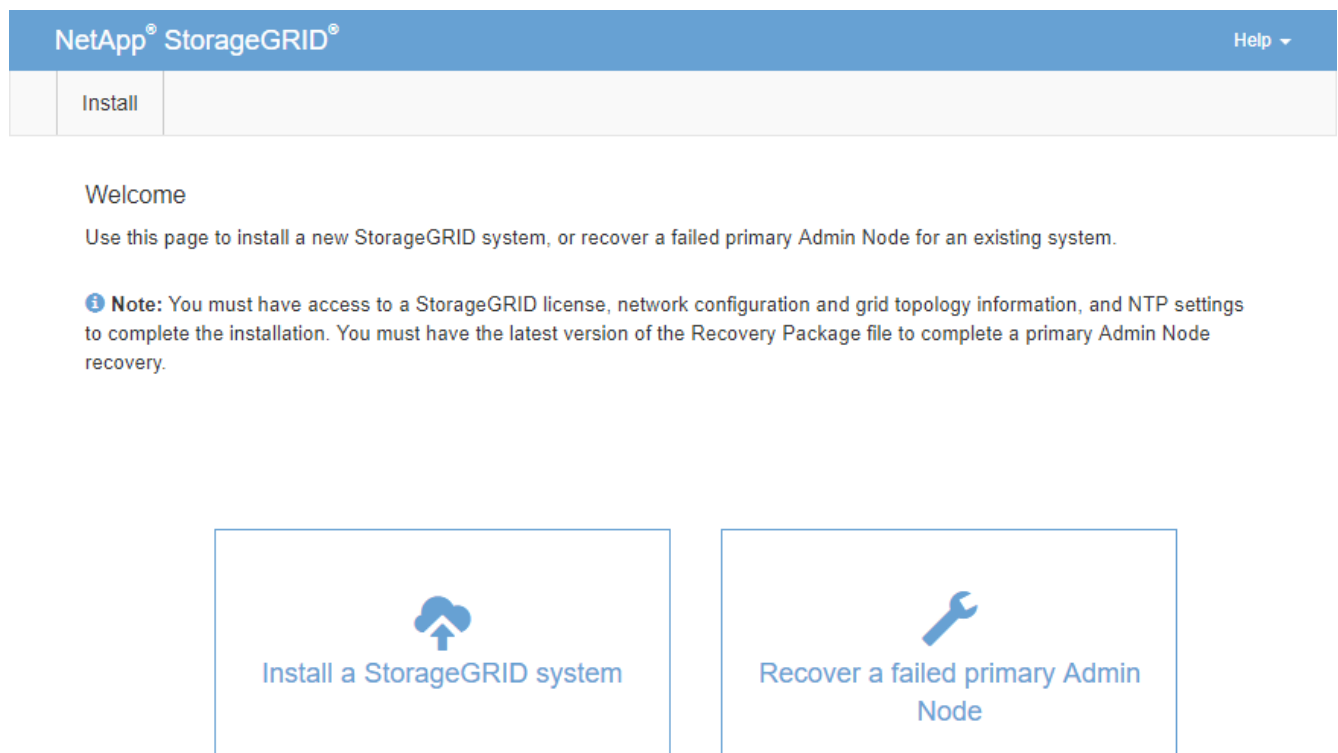
Avant de commencer

- Pour les nœuds d'administration principaux hébergés sur des machines virtuelles, la machine virtuelle a été déployée, mise sous tension et initialisée.
- Pour les nœuds d'administration primaires hébergés sur une appliance de services, vous avez remplacé l'appliance et installé le logiciel. Voir la ["instructions d'installation de votre appareil"](#).
- Vous disposez de la dernière sauvegarde du fichier du package de récupération(`sgws-recovery-package-id-revision.zip`).

- Vous avez la phrase secrète pour le provisionnement.

Étapes

1. Ouvrez votre navigateur Web et accédez à `https://primary_admin_node_ip`.
2. Gérer un mot de passe temporaire du programme d'installation selon les besoins :
 - Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez-le pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation
 - Pour les systèmes sans système d'exploitation, le mot de passe a été automatiquement importé à partir du fichier de configuration du nœud à l'adresse `/etc/storagegrid/nodes/<node_name>.conf`
 - Pour les VM, le mot de passe SSH/console a été automatiquement importé à partir des propriétés OVF
 - Si aucun mot de passe n'a été défini, définissez éventuellement un mot de passe pour sécuriser le programme d'installation de StorageGRID.
3. Sélectionnez **Récupérer un nœud d'administration principal défaillant**.



4. Téléchargez la sauvegarde la plus récente du package de récupération :
 - a. Sélectionnez **Parcourir**.
 - b. Localisez le fichier de package de récupération le plus récent pour votre système StorageGRID, puis sélectionnez **Ouvrir**.
5. Saisissez la phrase secrète pour le provisionnement.
6. Sélectionnez **Démarrer la récupération**.

Le processus de récupération commence. Le Grid Manager peut devenir indisponible pendant quelques

minutes lorsque les services requis démarrent. Une fois la récupération terminée, la page de connexion s'affiche.

7. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du nœud d'administration.



Pour configurer une approbation de partie de confiance, reportez-vous à la configuration de l'authentification unique (SSO) à l'aide de "OIDC" ou "SAML". Pour accéder au certificat serveur par défaut, connectez-vous au shell de commande du nœud d'administration. Accédez au répertoire `/var/local/mgmt-api`, puis sélectionnez le fichier `server.crt`.



Après la récupération d'un nœud d'administration principal, "[déterminez si vous devez appliquer un correctif](#)".

Déterminer l'exigence de correctif pour le nœud d'administration principal dans StorageGRID

Après avoir récupéré un nœud d'administration principal, déterminez si vous devez appliquer un correctif.

Avant de commencer

La restauration du nœud d'administration principal est terminée.

Étapes

1. Connectez-vous au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
2. Sélectionnez **Nœuds**.
3. Dans la liste de gauche, sélectionnez le nœud d'administration principal.
4. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.
5. Sélectionnez un autre nœud de grille.
6. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.
 - Si les versions affichées dans les champs **version du logiciel** sont identiques, vous n'avez pas besoin d'appliquer un correctif.
 - Si les versions affichées dans les champs **version du logiciel** sont différentes, vous devez "[appliquer un correctif](#)" mettre à jour le nœud d'administration principal récupéré avec la même version.

Restaurez le journal des audits sur le nœud d'administration principal StorageGRID récupéré.

Si vous avez pu conserver le journal d'audit à partir du nœud d'administration principal défaillant, vous pouvez le copier sur le nœud d'administration principal en cours de restauration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un nœud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.



Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :

- Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
- Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#) pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration restauré :

- a. Entrez la commande suivante : `ssh admin@recovery_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Une fois connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez quels fichiers d'audit ont été conservés : `cd /var/local/audit/export`

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration récupéré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.

5. Mettre à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration récupéré : `chown ams-user:bycast *`

6. Se déconnecter en tant que root : `exit`

Restaurez la base de données StorageGRID Admin Node lors de la récupération du nœud d'administration principal

Si vous souhaitez conserver les informations historiques relatives aux attributs et aux 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` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Données d'attributs historiques, utilisées dans les graphiques de style hérité de la page nœuds

Lorsque vous restaurez un nœud d'administration, le processus d'installation du logiciel crée une base de données de nœud d'administration vide sur le nœud récupéré. Toutefois, la nouvelle base de données comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un 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 primaire (le *source Admin Node*) vers le nœud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
3. Depuis le nœud d'administration source, arrêter le service Management application Program interface (mgmt-api) : `service mgmt-api stop`
4. Effectuez les étapes suivantes sur le nœud d'administration restauré :

- a. Connectez-vous au nœud d'administration restauré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- b. Arrêtez 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. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.
- f. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration restauré.

La base de données et ses données historiques sont copiées dans le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré.

- g. 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 StorageGRID

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration principal défaillant. Les metrics de Prometheus ne peuvent être restaurés que si votre système StorageGRID inclut un autre nœud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un nœud d'administration principal et que votre système StorageGRID dispose d'un autre nœud d'administration, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus à partir d'un nœud d'administration non primaire (le *source Admin Node*) vers le nœud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données Prometheus.



La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
 - a. Connectez-vous au nœud d'administration restauré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - b. Arrêtez le service Prometheus : `service prometheus stop`
 - c. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`
 - d. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.
 - 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 **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nœud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

- a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrer : `ssh-add -D`
4. Redémarrez le service Prometheus sur le nœud d'administration source. `service prometheus start`

Récupérez après des défaillances du nœud d'administration principal à l'aide d'un nœud d'administration non principal

Récupérez après une panne du nœud d'administration principal StorageGRID à l'aide d'un nœud d'administration non principal

Vous devez effectuer une série de tâches spécifiques pour récupérer suite à une panne du nœud d'administration principal à l'aide d'un nœud d'administration secondaire. Le nœud d'administration principal héberge le service Configuration Management Node (CMN) pour la grille.

Suivez ces étapes générales pour récupérer un nœud d'administration principal à l'aide d'un nœud d'administration non principal :

1. ["La copie des journaux d'audit à partir d'un nœud d'administration principal a échoué"](#)
2. ["Remplacez le nœud d'administration principal"](#)
3. ["Sélectionnez Démarrer la récupération pour configurer le nœud d'administration principal"](#)
4. ["Déterminez les exigences de correctif pour le nœud d'administration principal"](#)
5. ["Restaurez le journal d'audit sur le nœud d'administration principal restauré"](#)
6. ["Restaurez les metrics Prometheus lors de la récupération du nœud d'administration principal"](#)

Copiez les journaux d'audit StorageGRID à partir d'un nœud d'administration principal défaillant

Si vous pouvez copier les journaux d'audit à partir du nœud d'administration principal défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration principal restauré une fois qu'il est en cours d'exécution.

Description de la tâche

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.



Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

Étapes

1. Connectez-vous au nœud d'administration principal défaillant, si possible. Sinon, connectez-vous à n'importe quel nœud d'administration disponible.
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Saisissez la commande suivante pour passer au compte utilisateur root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal : `service ams stop`

3. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/audit/export
```

(ou `cd /var/local/log` sur les systèmes antérieurs)

4. Renommez le fichier journal source avec un nom de fichier numéroté unique.



- Si le fichier journal est dans le `/var/local/audit/export` répertoire, son nom est `audit.log`.
- Si le fichier journal est dans le `/var/local/log` répertoire, son nom est `localaudit.log`.

Par exemple, renommez le `localaudit.log` fichier à `2025-10-22.txt.1`.

```
ls -l  
mv localaudit.log 2025-10-22.txt.1
```

5. Redémarrez le service AMS : `service ams start`

6. Créez le répertoire pour copier tous les fichiers journaux d'audit dans 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 du compte utilisateur admin.

7. Copiez tous les fichiers journaux d'audit à 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 du compte utilisateur admin.

8. Déconnectez-vous en tant qu'utilisateur root : `exit`.

Remplacez le nœud d'administration principal StorageGRID à l'aide d'un nœud d'administration non principal

Pour restaurer 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 fonctionnant sur la même plateforme.
- Vous pouvez remplacer un nœud d'administration principal exécuté sur VMware ou un hôte Linux par un nœud d'administration principal hébergé sur une appliance de services StorageGRID.
- Vous pouvez remplacer un nœud d'administration principal exécuté sur un hôte VMware par un appliance

de services SG1000 ou SG100.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement des nœuds (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration du nœud d'administration principal.

Et de remplacement	Procédure
VMware	"Remplacer un nœud VMware par un nœud de récupération" "Remplacez le nœud VMware par une appliance de services SG1000 ou SG100."
Linux	"Remplacer un noeud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Ensuite, suivez la procédure pour " Remplacement d'un nœud Linux ".

Sélectionnez Démarrer la récupération pour configurer le nœud Admin principal

Après avoir remplacé un nœud d'administration principal, vous devez sélectionner Démarrer la récupération dans le Grid Manager pour configurer le nouveau nœud en remplacement du nœud défaillant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur web pris en charge](#)".
- Vous avez le "[Maintenance ou autorisation d'accès racine](#)".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Grid Manager, sélectionnez **Maintenance > Tasks > Node recovery**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la **phrase secrète de provisionnement**.
4. Sélectionnez **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. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.



Pendant la procédure de récupération, vous pouvez sélectionner **Réinitialiser** pour lancer une nouvelle récupération. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.

Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appliance à l'état pré-installé en l'exécutant `sgareinstall` sur le nœud. Voir ["Préparez l'appareil pour la réinstallation \(remplacement de la plate-forme uniquement\)"](#).

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du 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.

Déterminer l'exigence de correctif StorageGRID 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. Connectez-vous au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
2. Sélectionnez **Nœuds**.
3. Dans la liste de gauche, sélectionnez le nœud d'administration principal.
4. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.
5. Sélectionnez un autre nœud de grille.
6. Dans l'onglet Vue d'ensemble, notez les versions affichées dans le champ **Version du logiciel**.
 - Si les versions affichées dans les champs **version du logiciel** sont identiques, vous n'avez pas besoin d'appliquer un correctif.
 - Si les versions affichées dans les champs **version du logiciel** sont différentes, vous devez ["appliquer un correctif"](#) mettre à jour le nœud d'administration principal récupéré avec la même version.

Restaurez le journal des audits StorageGRID sur un nœud d'administration principal récupéré

Si vous avez pu conserver le journal d'audit à partir du nœud d'administration principal défaillant, vous pouvez le copier sur le nœud d'administration principal en cours de restauration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un nœud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :



- Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
- Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#) pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration restauré :

- a. Entrez la commande suivante : `ssh admin@recovery_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Une fois connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez quels fichiers d'audit ont été conservés : `cd /var/local/audit/export`

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration récupéré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
5. Mettre à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration récupéré : `chown ams-user:bycast *`
6. Se déconnecter en tant que root : `exit`

Restaurez les métriques Prometheus lors de la récupération d'un nœud d'administration principal StorageGRID

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration principal défaillant. Les metrics de Prometheus ne peuvent être restaurés que si votre système StorageGRID inclut un autre nœud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le

nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un nœud d'administration principal et que votre système StorageGRID dispose d'un autre nœud d'administration, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus à partir d'un nœud d'administration non primaire (le *source Admin Node*) vers le nœud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données Prometheus.



La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
 - a. Connectez-vous au nœud d'administration restauré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - b. Arrêtez le service Prometheus : `service prometheus stop`
 - c. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`
 - d. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.
 - 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 **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nœud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

- a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé

privée de l'agent SSH. Entrer :`ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration `source.service prometheus start`

Restaurez vos données en cas de défaillance d'un nœud d'administration non principal

Récupérer après des défaillances de nœuds d'administration non principaux StorageGRID

Vous devez effectuer les tâches suivantes pour effectuer une restauration à partir d'une panne de nœud d'administration non primaire. Un nœud d'administration héberge le service de nœud de gestion de la configuration (CMN) et est appelé nœud d'administration principal. Bien que vous puissiez avoir plusieurs nœuds d'administration, chaque système StorageGRID n'inclut qu'un seul nœud d'administration principal. Tous les autres nœuds d'administration sont des nœuds d'administration non primaires.

Pour restaurer un nœud d'administration non principal, procédez comme suit :

1. ["Copie des journaux d'audit à partir du nœud d'administration non principal en échec"](#)
2. ["Remplacez le nœud d'administration non principal"](#)
3. ["Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal"](#)
4. ["Restaurez le journal d'audit sur un nœud d'administration non principal restauré"](#)
5. ["Restaurez la base de données du nœud d'administration lors de la récupération d'un nœud d'administration non primaire"](#)
6. ["Restauration de metrics Prometheus lors de la restauration d'un nœud d'administration non principal"](#)

Copiez les journaux d'audit à partir d'un nœud d'administration non principal StorageGRID défaillant

Si vous pouvez copier les journaux d'audit depuis le nœud d'administration défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration non primaire restauré après son exécution.

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.



Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

1. Si possible, connectez-vous au nœud d'administration défaillant. Sinon, connectez-vous au nœud

d'administration principal ou à un autre nœud d'administration, le cas échéant.

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal : `service ams stop`
3. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/audit/export/
```

4. Renommez le fichier source `audit.log` en 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 dans un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

7. Copiez tous les fichiers journaux d'audit à l'emplacement temporaire : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

8. Se déconnecter en tant que root : `exit`

Remplacer le nœud d'administration non principal StorageGRID

Pour restaurer un nœud d'administration non primaire, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un nœud d'administration non primaire défaillant par un nœud d'administration non primaire exécuté sur la même plate-forme, ou remplacer un nœud d'administration non primaire exécuté sur VMware ou un hôte Linux par un nœud d'administration non primaire hébergé sur une appliance de services.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement de nœud (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration de nœud d'administration non primaire.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Ensuite, suivez la procédure pour "Remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal de StorageGRID

Après avoir remplacé un noeud d'administration non primaire, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Grid Manager, sélectionnez **Maintenance > Tasks > Node recovery**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la **phrase secrète de provisionnement**.
4. Sélectionnez **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. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.



Pendant la procédure de récupération, vous pouvez sélectionner **Réinitialiser** pour lancer une nouvelle récupération. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.

Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appliance à l'état pré-installé en l'exécutant `sgareinstall` sur le nœud. Voir ["Préparez l'appareil pour la réinstallation \(remplacement de la plate-forme uniquement\)"](#).

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du 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 des audits sur le nœud d'administration non principal StorageGRID récupéré

Si vous avez pu conserver le journal d'audit à partir du nœud d'administration non primaire défaillant, de sorte que les informations du journal d'audit historique soient conservées, vous pouvez le copier sur le nœud d'administration non primaire que vous

êtes en train de récupérer.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un nœud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.



Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :

- Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
- Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#) pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration restauré :

a. Entrez la commande suivante :

```
ssh admin@recovery_Admin_Node_IP
```

b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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 restauré :

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
5. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré :

```
chown ams-user:bycast *
```

6. Se déconnecter en tant que root : `exit`

Restaurez la base de données StorageGRID du nœud d'administration lors de la récupération d'un nœud d'administration non principal

Si vous souhaitez conserver les informations historiques relatives aux attributs et aux 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` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Données d'attributs historiques, utilisées dans les graphiques de la page Nœuds

Lorsque vous restaurez un nœud d'administration, le processus d'installation du logiciel crée une base de données de nœud d'administration vide sur le nœud récupéré. Toutefois, la nouvelle base de données comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un nœud d'administration non primaire, vous pouvez restaurer les informations d'historique en copiant la base de données 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 fonctions de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Exécutez la commande suivante depuis le nœud d'administration source. Saisissez ensuite la phrase secrète de provisionnement si vous y êtes invité. `recover-access-points`
3. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
4. Depuis le nœud d'administration source, arrêter le service Management application Program interface (mgmt-api) : `service mgmt-api stop`
5. Effectuez les étapes suivantes sur le nœud d'administration restauré :
 - a. Connectez-vous au nœud d'administration restauré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - b. Arrêtez 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. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.
 - f. 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`

Restaurez les métriques Prometheus lors de la récupération du nœud d'administration non principal de StorageGRID

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration non primaire qui a échoué.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un nœud d'administration non primaire, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus du nœud d'administration principal (le *source Admin Node*) vers le

noeud d'administration récupéré.



La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
 - a. Connectez-vous au nœud d'administration restauré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour basculer en root : `su -`
 - iv. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - b. Arrêtez le service Prometheus : `service prometheus stop`
 - c. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`
 - d. Entrez le mot de passe d'accès SSH indiqué dans le `Passwords.txt` fichier.
 - 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 **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le noeud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

- a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrer : `ssh-add -D`
4. Redémarrez le service Prometheus sur le nœud d'administration source. `service prometheus start`

Restaurez les données à partir d'une défaillance de nœud de passerelle

Remplacer le nœud de passerelle StorageGRID

Vous pouvez remplacer un nœud de passerelle défaillant par un nœud de passerelle exécuté sur le même matériel physique ou virtuel, ou remplacer un nœud de passerelle exécuté sur VMware ou un hôte Linux par un nœud de passerelle hébergé sur une appliance de services.

La procédure de remplacement des nœuds que vous devez suivre dépend de la plateforme à utiliser par le nœud de remplacement. Une fois la procédure de remplacement de nœud terminée, qui convient à tous les types de nœud, cette procédure vous dirige vers l'étape suivante pour la restauration du nœud de passerelle.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Ensuite, suivez la procédure pour "Remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle StorageGRID

Après avoir remplacé un noeud de passerelle, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez le ["Maintenance ou autorisation d'accès racine"](#).
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Grid Manager, sélectionnez **Maintenance > Tasks > Node recovery**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la **phrase secrète de provisionnement**.
4. Sélectionnez **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. Surveiller la progression de la récupération dans le tableau de nœuds de grille de récupération.



Pendant la procédure de récupération, vous pouvez sélectionner **Réinitialiser** pour lancer une nouvelle récupération. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.

Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appliance à l'état pré-installé en l'exécutant `sgareinstall` sur le nœud. Voir ["Préparez l'appareil pour la réinstallation \(remplacement de la plate-forme uniquement\)"](#).

Échec de la restauration à partir du nœud d'archivage

Récupérer après des pannes de nœuds d'archivage StorageGRID

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

Pour plus d'informations sur la récupération des nœuds d'archivage, reportez-vous à la section ["Restauration suite aux défaillances de nœud d'archivage \(site de documentation StorageGRID 11.8\)"](#).

Remplacez le nœud Linux

Remplacer un nœud Linux dans StorageGRID

Si une défaillance nécessite le déploiement d'un ou de plusieurs nouveaux hôtes

physiques ou virtuels ou la réinstallation de Linux sur un hôte existant, déployez et configurez l'hôte de remplacement avant de pouvoir restaurer le nœud de grille. Cette procédure constitue une étape du processus de restauration des nœuds grid pour tous les types de nœuds.

« Linux » fait référence à un déploiement Red Hat® Enterprise Linux® (RHEL), Ubuntu® ou Debian®. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Cette procédure n'est effectuée qu'en une seule étape du processus de restauration des nœuds de stockage logiciels, des nœuds d'administration principaux ou non primaires 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 restaurer les nœuds de grille dans n'importe quel ordre. Cependant, si le nœud d'administration principal est présent, vous devez le restaurer en premier afin d'éviter de bloquer la restauration des autres nœuds de grille lorsqu'ils essaient de contacter le nœud d'administration principal. Si vous ne pouvez pas restaurer le nœud d'administration principal en premier et qu'un nœud d'administration non principal est disponible, vous pouvez utiliser un nœud d'administration non principal pour restaurer les nœuds dans n'importe quel ordre.

Déployer de nouveaux hôtes Linux pour StorageGRID

À quelques exceptions près, vous préparez les nouveaux hôtes comme vous l'avez fait lors du processus d'installation initiale.

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. Voir "[Installez Linux](#)".



« Linux » fait référence à un déploiement RHEL, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp \(IMT\)](#)".

Cette procédure comprend les étapes permettant d'effectuer les tâches suivantes :

1. Installez Linux.
2. Configurez le réseau hôte.
3. Configurer le stockage de l'hôte
4. Installer le moteur de mise en conteneurs.
5. Installez le service hôte StorageGRID.



Arrêtez-vous une fois que vous avez terminé la tâche « installer le service hôte StorageGRID » dans les instructions d'installation. Ne lancez pas la tâche « déploiement des nœuds grid ».

À mesure que vous effectuez ces étapes, prenez note des consignes importantes suivantes :

- Veillez à utiliser les mêmes noms d'interface hôte que ceux utilisés sur l'hôte d'origine.
- Si vous utilisez un stockage partagé pour prendre en charge vos nœuds StorageGRID, ou si vous avez déplacé tout ou partie des disques ou disques SSD de vers les nœuds de remplacement, vous devez rétablir les mêmes mappages du stockage que ceux présents sur l'hôte d'origine. Par exemple, si vous

avez utilisé des WWID et des alias dans comme recommandé dans les `/etc/multipath.conf` instructions d'installation, veuillez à utiliser les mêmes paires alias/WWID dans `/etc/multipath.conf` sur l'hôte de remplacement.

- Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Restaurez les nœuds StorageGRID sur l'hôte

Pour restaurer un nœud de grille défaillant sur un nouvel hôte Linux, procédez comme suit afin de restaurer le fichier de configuration du nœud.

1. [Restaurer et valider le nœud](#) en restaurant le fichier de configuration du nœud. Pour une nouvelle installation, vous créez un fichier de configuration de nœud pour chaque nœud de grille à installer sur un hôte. Lors de la restauration d'un nœud de grille sur un hôte de remplacement, vous restaurez ou remplacez le fichier de configuration de nœud pour les nœuds de grille défaillants.
2. [Démarrez le service d'hôte StorageGRID](#).
3. Au besoin, [restaurez tous les nœuds qui ne démarrent pas](#).

Si des volumes de stockage en blocs ont été préservés à partir de l'hôte précédent, vous devrez peut-être effectuer des procédures de restauration supplémentaires. Les commandes de cette section vous aident à déterminer les procédures supplémentaires requises.

Restaurez et validez les nœuds de la grille

Si vous récupérez un nœud à partir d'un nœud d'administration non principal, définissez `ADMIN_IP` sur l'adresse IP du réseau Grid de ce nœud d'administration non principal, afin que le nœud récupéré s'enregistre auprès du nœud d'administration non principal plutôt qu'auprès du nœud d'administration principal. Pour consulter les règles relatives aux clés du réseau d'administration, reportez-vous à "[Créer des fichiers de configuration de nœud StorageGRID pour les déploiements Linux](#)".

Vous devez restaurer les fichiers de configuration de la grille de tout nœud de grille ayant échoué, puis valider les fichiers de configuration de la grille et résoudre les erreurs éventuelles.

Description de la tâche

Vous pouvez importer tout nœud de grille qui doit être présent sur l'hôte, tant que son `/var/local` volume n'a pas été perdu en raison de la défaillance de l'hôte précédent. Par exemple, ce `/var/local` volume peut toujours exister si vous avez utilisé le stockage partagé pour les volumes de données système StorageGRID, comme décrit dans les instructions d'installation de StorageGRID pour votre système d'exploitation Linux. L'importation du nœud restaure son fichier de configuration de nœud vers l'hôte.

S'il n'est pas possible d'importer des nœuds manquants, vous devez recréer leurs fichiers de configuration de grille.

Vous devez ensuite valider le fichier de configuration de la grille et résoudre tous les problèmes de réseau ou de stockage qui pourraient se produire avant de redémarrer StorageGRID. Lorsque vous recréez le fichier de configuration d'un nœud, vous devez utiliser le même nom pour le nœud de remplacement utilisé pour le

nœud en cours de restauration.

Voir le["Instructions d'installation de Linux"](#) pour plus d'informations sur l'emplacement du `/var/local` volume pour un nœud.

Étapes

- 1. Sur la ligne de commande de l'hôte restauré, répertorier 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 grid sont configurés, la sortie doit être au format suivant :

Name	Metadata-Volume
=====	
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Si certains ou tous les nœuds de grille qui doivent être configurés sur l'hôte ne sont pas répertoriés, vous devez restaurer les nœuds de grille manquants.

- 2. Pour importer des nœuds de grille ayant 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`

La `storagegrid node import` commande réussit uniquement si le nœud cible a été arrêté correctement sur l'hôte sur lequel il a été exécuté en dernier. Si ce n'est pas le cas, vous observez une erreur semblable à ce qui suit :

`This node (node-name) appears to be owned by another host (UUID host-uuid).`

Use the `--force` flag if you are sure import is safe.

- a. Si une erreur s'est produite au sujet du nœud appartenant à un autre hôte, exécutez de nouveau la commande avec `--force` l'indicateur pour terminer l'importation :`sudo storagegrid --force node import node-var-local-volume-path`



Tous les nœuds importés avec l' `--force` indicateur nécessitent des étapes de récupération supplémentaires avant de pouvoir rejoindre la grille, comme décrit dans ["Qu'est-ce qui suit : effectuez d'autres étapes de restauration, le cas échéant"](#).

- 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["Créez des fichiers de configuration de nœud"](#) .



Lorsque vous recréez le fichier de configuration d'un nœud, vous devez utiliser le même nom pour le nœud de remplacement utilisé pour le nœud en cours de restauration. Pour les déploiements Linux, assurez-vous que le nom du fichier de configuration contient le nom du nœud. Lorsque cela est possible, vous devez utiliser les mêmes interfaces réseau, les mêmes mappages de périphériques de bloc et les mêmes adresses IP. Cette pratique réduit la quantité de données à copier sur le nœud lors de la restauration, ce qui peut accélérer la restauration (dans certains cas, quelques minutes au lieu de plusieurs semaines).



Si vous utilisez de nouveaux périphériques de bloc (périphériques que le nœud StorageGRID n'a pas utilisés auparavant) comme valeurs pour l'une des variables de configuration commençant par `BLOCK_DEVICE_` lorsque vous recréez le fichier de configuration d'un nœud, suivez les instructions de la section [Corrigez les erreurs de périphérique de bloc manquantes](#).

4. Exécutez la commande suivante sur l'hôte restauré pour lister tous les nœuds StorageGRID.

```
sudo storagegrid node list
```

5. Valider le fichier de configuration de nœud pour chaque nœud de la grille dont le nom s'affiche dans la sortie de la liste des nœuds StorageGRID :

```
sudo storagegrid node validate node-name
```

Vous devez corriger toute erreur ou avertissement avant de démarrer le service hôte StorageGRID. Les sections suivantes donnent plus de détails sur les erreurs susceptibles d'avoir une importance particulière pendant la récupération.

Corrigez les erreurs d'interface réseau manquantes

Si le réseau hôte n'est pas configuré correctement ou si un nom est mal orthographié, une erreur se produit lorsque StorageGRID vérifie le mappage spécifié dans le `/etc/storagegrid/nodes/node-name.conf` fichier.

Une erreur ou un avertissement correspondant à ce modèle peut s'afficher :

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

L'erreur peut être signalée pour le réseau Grid, le réseau Admin ou le réseau client. Cette erreur signifie que le `/etc/storagegrid/nodes/node-name.conf` fichier mappe le réseau StorageGRID indiqué sur l'interface hôte nommée `host-interface-name`, mais qu'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 de la section "[Déploiement de nouveaux hôtes Linux](#)". Utilisez les mêmes noms pour toutes les interfaces hôtes que ceux utilisés sur l'hôte d'origine.

Si vous ne parvenez pas à nommer les interfaces hôtes pour qu'elles correspondent au fichier de configuration du nœud, vous pouvez modifier le fichier de configuration du nœud et modifier la valeur de `GRID_NETWORK_TARGET`, `ADMIN_NETWORK_TARGET` ou `client_NETWORK_TARGET` pour qu'elle

corresponde à une interface hôte existante.

Assurez-vous que l'interface hôte donne accès au port réseau physique ou au VLAN approprié et que l'interface ne fait pas directement référence à un périphérique de liaison ou de pont. Vous devez soit configurer un VLAN (soit une autre interface virtuelle) sur le périphérique de liaison de l'hôte, soit utiliser un pont et une paire Ethernet virtuelle (veth).

Corrigez les erreurs de périphérique de bloc manquantes

Le système vérifie que chaque nœud récupéré est associé à un fichier spécial de périphérique de bloc valide ou à un lien logiciel valide vers un fichier spécial de périphérique de bloc. Si StorageGRID trouve un mappage non valide dans le `/etc/storagegrid/nodes/node-name.conf` fichier, une erreur de périphérique de bloc manquant s'affiche.

Si vous observez une erreur correspondant à ce modèle :

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Cela signifie que `/etc/storagegrid/nodes/node-name.conf` mappe le périphérique de bloc utilisé par *nom-nœud* pour `PURPOSE` au nom-chemin donné dans le système de fichiers Linux, mais qu'il n'existe pas de fichier spécial de périphérique de bloc valide, ou de lien logiciel vers un fichier spécial de périphérique de bloc, à cet emplacement.

Vérifiez que vous avez effectué les étapes de la section "[Déploiement de nouveaux hôtes Linux](#)". Utilisez les mêmes noms de périphériques persistants pour tous les périphériques de bloc que ceux utilisés sur l'hôte d'origine.

Si vous ne parvenez pas à restaurer ou à recréer le fichier spécial de périphérique de bloc manquant, vous pouvez attribuer un nouveau périphérique de bloc de la taille et de la catégorie de stockage appropriées et modifier le fichier de configuration de nœud pour modifier la valeur de `BLOCK_DEVICE_PURPOSE` à pointer vers le nouveau fichier spécial de périphérique de bloc.

Déterminez la taille et la catégorie de stockage appropriées à l'aide des tableaux correspondant à votre système d'exploitation Linux. Voir "[Les besoins en matière de stockage et de performances](#)".

Consultez les recommandations pour "[configuration du stockage hôte](#)" avant de procéder au remplacement du dispositif de blocage.



Si vous devez fournir un nouveau périphérique de stockage en mode bloc pour l'une des variables de fichier de configuration commençant par `BLOCK_DEVICE_` parce que le périphérique de bloc d'origine a été perdu avec l'hôte en panne, assurez-vous que le nouveau périphérique de bloc n'est pas formaté avant de tenter d'autres procédures de récupération. Le nouveau périphérique de bloc n'est pas formaté si vous utilisez un stockage partagé et que vous avez créé un nouveau volume. Si vous n'êtes pas certain, exécutez la commande suivante sur tout nouveau fichier spécial de périphérique de stockage en mode bloc.



Exécutez la commande suivante uniquement pour les nouveaux périphériques de stockage en mode bloc. N'exécutez pas cette commande si vous pensez que le stockage en mode bloc contient toujours des données valides pour le nœud en cours de restauration, car toutes les données du périphérique seront perdues.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Démarrez le service d'hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et s'assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid  
sudo systemctl start storagegrid
```

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

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

3. Si l'un des nœuds 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
```

Restaurez les nœuds qui ne démarrent pas normalement

Si un nœud StorageGRID ne rejoint pas la grille normalement et qu'il n'apparaît pas comme récupérable, il est possible qu'il soit corrompu. Vous pouvez forcer le nœud en mode de récupération.

Étapes

1. Vérifiez que la configuration réseau du nœud est correcte.

Le nœud n'a peut-être pas pu rejoindre la grille en raison de mappages d'interface réseau incorrects ou d'une adresse IP ou d'une passerelle de réseau Grid incorrecte.

2. Si la configuration réseau est correcte, lancer la `force-recovery` commande :

```
sudo storagegrid node force-recovery node-name
```

3. Effectuez les étapes de restauration supplémentaires pour le nœud. Voir ["Qu'est-ce qui suit : effectuez d'autres étapes de restauration, le cas échéant"](#).

Effectuez des étapes de récupération supplémentaires du nœud StorageGRID

En fonction des actions spécifiques que vous avez effectuées pour exécuter les nœuds StorageGRID sur l'hôte de remplacement, vous devrez peut-être effectuer des étapes de restauration supplémentaires pour chaque nœud.

La récupération de nœud est terminée si vous n'avez pas besoin d'effectuer d'actions correctives pendant que vous avez remplacé l'hôte Linux ou restauré le nœud de grille défaillant vers le nouvel hôte.

Actions correctives et étapes suivantes

Lors du remplacement d'un nœud, vous devrez peut-être effectuer l'une des actions correctives suivantes :

- Vous devez utiliser l' `--force` indicateur pour importer le nœud.
- Pour tout `<PURPOSE>`, la valeur de la `BLOCK_DEVICE_<PURPOSE>` variable de fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant la défaillance de l'hôte.
- Vous avez émis `storagegrid node force-recovery node-name` pour le nœud.
- Vous avez ajouté un nouveau périphérique de bloc.

Si vous avez pris **l'une** de ces actions correctives, vous devez effectuer des étapes de récupération supplémentaires.

Type de restauration	Étape suivante
Nœud d'administration principal	• "Sélectionnez Démarrer la récupération pour configurer le nœud Admin principal" • "Récupérez le nœud d'administration principal à l'aide d'un nœud d'administration non principal"
Nœud d'administration non primaire	"Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire"
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"

Type de restauration	Étape suivante
Nœud de stockage (basé sur logiciel) : • Si vous deviez utiliser l'indicateur pour importer le nœud, ou si <code>--force</code> 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 restauration pour configurer le nœud de stockage"
Nœud de stockage (basé sur logiciel) : • Si vous avez ajouté un nouveau périphérique de bloc. • Si, pour n'importe quel <code><PURPOSE></code>, la valeur de la <code>BLOCK_DEVICE_<PURPOSE></code> variable de fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant la défaillance de l'hôte.	"Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact"

Remplacez un nœud VMware dans StorageGRID par un nœud de récupération

Lorsque vous restaurez un nœud StorageGRID en panne hébergé sur VMware, vous supprimez le nœud en panne et déployez un nœud de restauration.

Avant de commencer

Vous avez déterminé que la machine virtuelle ne peut pas être restaurée et doit être remplacée.

Description de la tâche

Utilisez le client Web VMware vSphere pour supprimer d'abord la machine virtuelle associée au nœud de grille défaillant. Vous pouvez ensuite déployer une nouvelle machine virtuelle.

Cette procédure ne représente qu'une étape du processus de restauration du nœud grid. La procédure de retrait 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 au client Web VMware vSphere.
2. Accédez à la machine virtuelle du nœud de grille qui a échoué.
3. Notez toutes les informations nécessaires au déploiement du nœud de restauration.
 - a. Cliquez avec le bouton droit de la souris sur la machine virtuelle, sélectionnez l'onglet **Modifier les paramètres** et notez les paramètres utilisés.
 - b. Sélectionnez l'onglet **vApp Options** pour afficher et enregistrer les paramètres réseau du nœud de grille.
4. Si le nœud de grille défaillant est un nœud de stockage, déterminez si l'un des disques durs virtuels utilisés pour le stockage des données n'est pas endommagé et conservez-le pour qu'il soit reconnecté au nœud de grille récupéré.
5. Mise hors tension de la machine virtuelle

6. Sélectionnez **actions > toutes les actions vCenter > Supprimer du disque** pour supprimer la machine virtuelle.
7. Déployez une nouvelle machine virtuelle 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 remappage les ports de nœud ou augmenter les paramètres de processeur ou de mémoire.



Après le déploiement du nouveau nœud, vous pouvez ajouter de nouveaux disques virtuels en fonction de vos besoins de stockage, rattacher tout disque dur virtuel conservé à partir du nœud de grille défaillant précédemment retiré, ou les deux.

8. Suivez la procédure de restauration des nœuds, en fonction du type de nœud que vous restaurez.

Type de nœud	Accédez à
Nœuds d'administration	" Récupération du nœud d'administration principal ou non principal dans StorageGRID "
Nœud de passerelle	" Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle "
Nœud de stockage	" Sélectionnez Démarrer la restauration pour configurer le nœud de stockage "

Remplacez le nœud VMware dans StorageGRID par SG1000 ou SG100

Si le nœud d'administration principal fonctionne en tant que nœud VMware, vous pouvez le remplacer par un appliance de services SG1000 ou SG100.



Une fois le remplacement du nœud effectué et vérifié, vous devez supprimer le nœud VMware d'origine. Le maintien de l'ancien nœud en place risque une perturbation majeure du grid s'il est remis en ligne.

Avant de commencer

- Vous avez déterminé que la machine virtuelle ne peut pas être restaurée et doit être remplacée.
- Vous avez vérifié qu'aucune opération de maintenance du grid n'est en cours.
- Vous avez confirmé que la version de l'installateur de l'appliance StorageGRID sur l'appliance de services SG1000 ou SG100 correspond à la version logicielle de votre système StorageGRID.
- Vous disposez des informations suivantes concernant le nœud d'administration principal existant :

Nom du nœud : Vous devez installer le dispositif de services en utilisant le même nom de nœud que le nœud d'administration principal existant. Le nom du nœud correspond au nom d'hôte (nom du système).

Adresse IP : Vous pouvez attribuer au dispositif de services la même adresse IP que le nœud d'administration principal existant (recommandé), ou vous pouvez sélectionner une nouvelle adresse IP

inutilisée sur chaque réseau.

- Vous avez la phrase secrète pour le provisionnement.

Étape 1 : Remplacez le nœud VMware

Commencez par supprimer le nœud d'administration principal existant dans le Grid Manager. Ensuite, vous installez l'appliance de services SG1000 ou SG100 comme nouveau nœud d'administration principal à l'aide de StorageGRID Appliance Installer, puis vous restaurez le nœud. Si vous utilisez une nouvelle adresse IP, vous pouvez installer l'appliance de services avant de supprimer le nœud d'administration principal existant.

Utiliser l'adresse IP existante

Remplacez le nœud d'administration principal en utilisant l'adresse IP du nœud d'administration principal existant.

Étapes

1. Téléchargez le package de récupération depuis le Grid Manager :
 - a. Sélectionnez **Maintenance > Recovery package**.
 - b. Saisissez la phrase secrète de provisionnement et téléchargez le package.
2. Connectez-vous au nœud d'administration principal existant :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Passez en mode root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

3. ["Copiez les journaux d'audit du nœud d'administration principal existant"](#).
4. Arrêtez Server Manager et tous les services sur le nœud de la grille :

```
shutdown -h now
```

Veuillez prévoir jusqu'à 15 minutes pour l'arrêt des services.

5. ["Installez l'appareil de services SG1000 ou SG100"](#).
6. ["Déployez l'appliance de services SG1000 ou SG100"](#).
7. Après avoir sélectionné **Démarrer l'installation**, veuillez prévoir environ dix minutes pour que l'installation atteigne l'étape **Charger l'installateur StorageGRID**.

Au bout de six à sept minutes, le navigateur redirige pour démarrer la récupération.

8. Vérifiez que l'horloge de l'appareil est correcte.
 - a. Utilisez SSH pour vous connecter au port 8022 :
 - i. Saisissez la commande : `ssh -p 8022 admin@grid_node_IP`.
 - ii. Passez en mode root : `su -`
 - iii. Saisissez `netappl!`.
 - b. Vérifiez que l'horloge de l'appareil est à quelques minutes près de l'heure UTC actuelle. Si nécessaire, réglez la date et l'heure correctes.

```
date -s "DD Mon YYYY HH:MM:SS"
```

9. Retournez dans votre navigateur Web et sélectionnez **Récupérer un nœud d'administration principal défaillant**.

10. Téléversez le [package de récupération que vous avez téléchargé](#).
11. Saisissez la phrase secrète de provisionnement et sélectionnez **Démarrer la récupération**.

La barre de progression de la récupération s'affiche. Prévoyez six à dix minutes pour que le processus de récupération se termine et que les services démarrent.

12. Connectez-vous à Grid Manager lorsque vous y êtes invité.

Utiliser une nouvelle adresse IP

Remplacez le nœud d'administration principal en utilisant une nouvelle adresse IP.

Étapes

1. "Installez l'appareil de services SG1000 ou SG100".
2. Vérifiez que l'horloge de l'appareil est correcte afin d'éviter les erreurs NTP pendant la récupération.
 - a. Utilisez SSH pour vous connecter au port 8022 :
 - i. Saisissez la commande : `ssh -p 8022 admin@grid_node_IP`.
 - ii. Passez en mode root : `su -`
 - iii. Saisissez `netapp1!`.
 - b. Vérifiez que l'horloge de l'appareil est à quelques minutes près de l'heure UTC actuelle. Si nécessaire, réglez la date et l'heure correctes.

```
date -s "DD Mon YYYY HH:MM:SS"
```

3. Accédez à **Upload StorageGRID Software** dans le StorageGRID Appliance Installer et vérifiez que la version du logiciel préinstallée sur l'appliance correspond à la version de StorageGRID en cours d'exécution sur la grille. Si les versions ne correspondent pas :
 - a. Téléchargez le package d'installation Debian StorageGRID approprié depuis le ["Site de support NetApp"](#).
 - b. Sélectionnez **Supprimer** pour supprimer le logiciel d'installation.
 - c. Téléversez les fichiers `storagegrid-webscale-images-<sg-version>.deb` et `storagegrid-webscale-images-<sgversion>.deb.md5`.
4. Dans l'onglet Accueil de l'installateur d'appliance StorageGRID, sélectionnez **Primary Admin (with Load Balancer)** comme type de nœud.
5. Saisissez le nom du nœud. Le nom du nœud doit correspondre au nom du nœud d'administration principal existant.



Ne sélectionnez pas **Démarrer l'installation**.

6. Vérifiez si le sous-réseau de la nouvelle adresse IP est présent dans le réseau grid. Si le nouveau sous-réseau IP n'est pas présent, ajoutez-le au réseau grid :
 - a. Dans Grid Manager, sélectionnez **Maintenance > Grid Network**.
 - b. Saisissez la phrase secrète de provisionnement pour mettre à jour la liste des sous-réseaux.
7. Téléchargez le package de récupération depuis GRID Manager :
 - a. Sélectionnez **Maintenance > Recovery package**.

b. Saisissez la phrase secrète de provisionnement, puis téléchargez le package.

8. Connectez-vous au nœud d'administration principal existant :

a. Entrez la commande suivante : `ssh admin@grid_node_IP`

b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour basculer en root : `su -`

d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

9. "[Copiez les journaux d'audit du nœud d'administration principal existant](#)".

10. Arrêtez Server Manager et tous les services sur le nœud de la grille :

```
service servermanager stop
```

Veuillez prévoir jusqu'à 15 minutes pour l'arrêt des services.

11. Sur l'onglet Accueil de l'installateur d'appliance StorageGRID :

a. Vérifiez les paramètres suivants :

- Le type de nœud est défini sur **Primary Admin (with Load Balancer)**
- Le nom du nœud correspond au nom du nœud d'administration principal existant

b. Notez la nouvelle adresse IP.

12. Sélectionnez **Démarrer l'installation**.

Prévoyez environ 10 minutes pour que l'installation atteigne l'étape **Load StorageGRID installer**.

Au bout de six à sept minutes, le navigateur redirige pour commencer la procédure de récupération.

13. Vérifiez que l'horloge de l'appareil est correcte.

a. Utilisez SSH pour vous connecter au port 8022 :

i. Saisissez la commande : `ssh -p 8022 admin@grid_node_IP`.

ii. Passez en mode root : `su -`

iii. Saisissez `netapp1!`.

b. Vérifiez que l'horloge de l'appareil est à quelques minutes près de l'heure UTC actuelle. Si nécessaire, réglez la date et l'heure correctes.

```
date -s "DD Mon YYYY HH:MM:SS"
```

14. Retournez au navigateur Web, puis sélectionnez **Récupérer un nœud d'administration principal défaillant**.

15. Téléversez le [package de récupération que vous avez téléchargé](#).

16. Saisissez la phrase secrète de provisionnement et sélectionnez **Démarrer la récupération**.

La page de récupération du nœud d'administration principal disparaît, puis réapparaît. Si vous sélectionnez **Démarrer la récupération** à nouveau, un 500: Internal Server Error apparaît car la récupération a commencé mais ne peut pas envoyer la mise à jour au Grid Manager, qui utilise la nouvelle adresse IP. Résolvez ce problème en mettant à jour l'adresse IP du nœud d'administration principal dans le fichier `/etc/hosts` :

- a. Utilisez SSH pour vous connecter au port 8022 :
 - i. Saisissez la commande : `ssh -p 8022 admin@grid_node_IP`.
 - ii. Passez en mode root : `su -`
 - iii. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- b. Accédez au journal :

```
tail /var/local/log/install.log
```

Vous devriez voir l'erreur suivante se répéter : `curl: (7) Failed to connect to <primary_Admin_Node_name> port9999: No route to host`

Il s'agit du comportement attendu. StorageGRID tente d'envoyer la mise à jour au nœud d'administration principal en utilisant l'adresse IP existante du nœud d'administration principal.

- c. Vérifiez que le conteneur est en cours d'exécution :

```
storagegrid node status
```

```
storagegrid node enter <primary_Admin_Node_name>
```

- a. Dans le fichier `/etc/hosts` à l'intérieur du conteneur, remplacez l'adresse IP du nœud d'administration principal existante par la nouvelle adresse IP.
- b. Enregistrez le fichier.
- c. Retournez au navigateur web. Après quelques secondes, la barre de progression de la récupération apparaît.

Veuillez prévoir six à dix minutes pour que le processus de récupération soit terminé et que les services démarrent.

17. Connectez-vous à Grid Manager lorsque vous y êtes invité.

18. Mettre à jour le package de récupération :

- a. Connectez-vous au nœud d'administration principal :
 - i. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - ii. Passez en mode root : `su -`
 - iii. Saisissez la commande suivante : `change-ip`
- b. Sélectionnez l'option **3 – Modifier les listes de sous-réseaux du réseau d'administration**, puis ajoutez le nouveau sous-réseau.

StorageGRID génère automatiquement un nouveau package de récupération avec la nouvelle adresse IP du nœud Admin principal.

Étape 2 : Terminez la récupération du nœud

Utilisez un nœud d'administration non principal existant comme nœud d'administration source pour les procédures de restauration (journal des audits, base de données du nœud d'administration et métriques Prometheus). Si la grille ne comporte aucun nœud d'administration non principal, vous pouvez utiliser le nœud VMware d'origine qui est remplacé, à condition qu'il s'exécute sur une adresse IP différente de celle du nœud d'administration principal restauré.

Étapes

1. ["Restaurez le journal des audits"](#).
2. ["Restaurez la base de données de l'Admin Node"](#).
3. ["Restaurer les métriques Prometheus"](#).
4. Vérifiez que le nouveau nœud d'administration principal fonctionne correctement. Ensuite, supprimez immédiatement le nœud de machine virtuelle ou le conteneur bare-metal d'origine.

Remplacez le nœud défectueux par l'appliance de services

Remplacez le nœud StorageGRID défaillant par un dispositif de services

Vous pouvez utiliser une appliance de services pour restaurer 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 une appliance de services. Cette procédure constitue une étape de la procédure de restauration des nœuds de la grille.

Avant de commencer

- Vous avez déterminé que l'une des situations suivantes est vraie :
 - Impossible de restaurer la machine virtuelle hébergeant le nœud.
 - L'hôte Linux physique ou virtuel du nœud grid a échoué et doit être remplacé.
 - L'appliance de services qui héberge le nœud de grid doit être remplacée.
- Vous avez confirmé que la version du programme d'installation de l'appliance StorageGRID installée sur l'appliance de services correspond à la version logicielle de votre système StorageGRID. Voir ["Vérifiez et mettez à niveau la version du programme d'installation de l'appliance StorageGRID"](#).



Ne déployez pas à la fois une appliance de services SG110 et SG1100 ou une appliance de services SG100 et SG1000 sur le même site. Cela peut entraîner des performances imprévisibles.

Description de la tâche

Vous pouvez utiliser une appliance de services pour restaurer un nœud de grille défaillant dans les cas suivants :

- Le nœud défaillant était hébergé sur VMware ou Linux (["changement de plateforme"](#))
- Le nœud défaillant était hébergé sur une appliance de services (["remplacement de la plate-forme"](#))

Installer l'appliance de services StorageGRID (changement de plateforme uniquement)

Lorsque vous récupérez un nœud de grid en panne hébergé sur VMware ou un hôte Linux et que vous utilisez une appliance de services pour le nœud de remplacement, vous devez d'abord installer le nouveau matériel de l'appliance en utilisant le même nom de nœud (nom du système) que le nœud en panne.

Avant de commencer

Vous disposez des informations suivantes sur le nœud défaillant :

- **Nom du nœud** : vous devez installer l'appliance 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 à l'appliance de services les mêmes adresses IP que le nœud défaillant, qui est l'option préférée, ou sélectionner une nouvelle adresse IP inutilisée sur chaque réseau.

Description de la tâche

Effectuez cette procédure uniquement si vous récupérez un nœud défaillant hébergé sur VMware ou Linux et que vous le remplacez par un nœud hébergé sur une appliance de services.

Étapes

1. Suivez les instructions d'installation d'une nouvelle appliance de services. Voir "[Démarrage rapide pour l'installation du matériel](#)".
2. Lorsqu'un nom de nœud est demandé, utilisez le nom du nœud correspondant à l'échec.

Préparez l'appliance StorageGRID pour la réinstallation (remplacement de la plateforme uniquement)

Lorsque vous récupérez un nœud de grid hébergé sur une appliance de services, vous devez d'abord préparer l'appliance pour la réinstallation du logiciel StorageGRID.

Effectuez cette procédure uniquement si vous remplacez un nœud défaillant hébergé sur une appliance de services. Ne suivez pas ces étapes si le nœud défaillant était initialement hébergé sur un hôte VMware ou Linux.

Étapes

1. Connectez-vous au nœud de grille ayant échoué :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Préparez l'appliance pour l'installation du logiciel StorageGRID. Entrer : `sgareinstall`
3. Lorsque vous êtes invité à continuer, entrez : `y`

L'appliance redémarre et votre session SSH se termine. La disponibilité du programme d'installation de

l'appliance StorageGRID prend généralement 5 minutes environ, même si dans certains cas, vous devrez attendre jusqu'à 30 minutes.

L'appliance de services est réinitialisée et les données du nœud grid n'sont plus accessibles. Les adresses IP configurées pendant le processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cette opération une fois la procédure terminée.

Une fois la commande exécutée `sgareinstall`, tous les comptes, mots de passe et clés SSH provisionnés par StorageGRID sont supprimés et de nouvelles clés hôte sont générées.

Démarrez l'installation du logiciel StorageGRID sur un appareil de services

Pour installer un nœud de passerelle ou un nœud d'administration sur une appliance de services, utilisez le programme d'installation de l'appliance StorageGRID, inclus dans l'appliance.

Avant de commencer

- L'appliance est installée dans un rack, connectée à vos réseaux et sous tension.
- Les liaisons réseau et les adresses IP sont configurées pour l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.
- Si vous installez un nœud de passerelle ou un nœud d'administration non principal, vous connaissez l'adresse IP de l'un des nœuds d'administration suivants :
 - Le nœud d'administration principal de la grille StorageGRID
 - Un nœud d'administration non principal, s'il en existe un et s'il est utilisé pour récupérer le nœud
- Si vous récupérez un nœud (y compris le nœud d'administration principal) en utilisant un nœud d'administration non principal, vous pouvez spécifier l'adresse IP de ce nœud d'administration.
- Tous les sous-réseaux de réseau de la grille répertoriés sur la page Configuration IP du programme d'installation de l'appliance StorageGRID sont définis dans la liste de sous-réseaux de réseau de la grille sur le nœud d'administration principal.

Voir ["Démarrage rapide pour l'installation du matériel"](#).

- Vous utilisez un ["navigateur web pris en charge"](#).
- L'une des adresses IP est attribuée à l'appliance. Vous pouvez utiliser l'adresse IP du réseau Admin, du réseau Grid ou du réseau client.
- Si vous installez un nœud d'administration principal, vous disposez des fichiers d'installation Ubuntu ou Debian pour cette version de StorageGRID.



Une version récente du logiciel StorageGRID est préchargée sur l'appliance de services pendant la fabrication. Si la version préchargée du logiciel correspond à la version utilisée dans votre déploiement StorageGRID, vous n'avez pas besoin des fichiers d'installation.

Description de la tâche

Pour installer le logiciel StorageGRID sur une appliance de services :

- Pour un nœud d'administration principal, vous spécifiez le nom du nœud, puis vous téléchargez les paquets logiciels appropriés (si nécessaire). Si vous restaurez le nœud d'administration principal et que vous disposez d'un nœud d'administration non principal dans votre grid, vous avez la possibilité soit de

restaurer le nœud à l'aide d'un nœud d'administration non principal en spécifiant l'adresse IP de ce nœud d'administration, soit d'installer ou de restaurer le nœud en utilisant votre configuration actuelle.

- Pour un nœud d'administration non primaire 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.
- Partway tout au long du processus, l'installation se met en pause. Pour reprendre l'installation, vous devez vous connecter à Grid Manager et configurer le nœud en attente en remplacement du nœud ayant échoué.
- Une fois le nœud configuré, le processus d'installation de l'appliance est terminé et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP de l'appliance de services.

`https://Controller_IP:8443`

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Pour installer un nœud d'administration principal :
 - a. Dans la section nœud, pour **Type de nœud**, sélectionnez **Administrateur principal**.
 - b. Dans le champ **Nom du nœud**, saisissez le même nom que celui utilisé pour le nœud que vous récupérez, puis sélectionnez **Enregistrer**.
 - c. Choisissez le mode approprié parmi les deux disponibles dans la section Mode d'installation. Vous pouvez sélectionner soit la méthode « Install a node or recover this node using current configuration », soit la méthode « Recover this node using a non-primary Admin Node ».

Méthode de configuration actuelle

Installez un nœud ou récupérez ce nœud en utilisant la configuration actuelle.

- i. Dans la section Installation, vérifiez la version du logiciel indiquée sous État actuel. Si la version du logiciel prêt à être installé est correcte, passez à la [Étape d'installation](#).
- ii. Si vous devez charger une autre version du logiciel, dans le menu **Avancé**, sélectionnez **Charger le logiciel StorageGRID**. La page Charger le logiciel StorageGRID s'affiche.
- iii. Sélectionnez **Parcourir** pour télécharger le **package logiciel** et le **fichier de somme de contrôle** pour le logiciel StorageGRID. Les fichiers sont automatiquement téléchargés après que vous les avez sélectionnés.
- iv. Sélectionnez **Accueil** pour revenir à la page d'accueil de l'installateur StorageGRID Appliance.

Méthode du nœud d'administration non principal

Récupérez ce nœud à l'aide d'un nœud d'administration non principal.

- i. Dans le champ Adresse IP du nœud d'administration non principal, saisissez l'adresse IP du réseau de la grille du nœud d'administration non principal que vous souhaitez utiliser pour la récupération, puis sélectionnez **Enregistrer**.
- ii. Si la version du logiciel prêt à être installée est correcte, passez directement à l' [Étape d'installation](#).

3. Pour installer un nœud de passerelle ou un nœud d'administration non principal :

- Dans la section noeud, pour **Type de noeud**, sélectionnez **passerelle** ou **non-administrateur principal**, selon le type de noeud que vous restaurez.
- Dans le champ **Nom du nœud**, saisissez le même nom que celui utilisé pour le nœud que vous récupérez, puis sélectionnez **Enregistrer**.
- Dans la section connexion au noeud d'administration principal, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

Le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

- Si cette adresse IP n'est pas affichée ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	- Décochez la case Activer la découverte du noeud d'administration. - Saisissez l'adresse IP manuellement. - Sélectionnez Enregistrer. - Patiencez pendant que l'état de connexion de la nouvelle adresse IP devient « prêt ».
Détection automatique de tous les nœuds d'administration principaux connectés	- Cochez la case Activer la découverte du noeud d'administration. - Dans la liste des adresses IP découvertes, sélectionnez le nœud d'administration principal de la grille sur lequel cette appliance de services sera déployée. - Sélectionnez Enregistrer. - Patiencez pendant que l'état de connexion de la nouvelle adresse IP devient « prêt ».

- dans la section installation, vérifiez que l'état actuel est prêt à démarrer l'installation du nom du noeud et que le bouton **Démarrer l'installation** est activé.

Si le bouton **Démarrer l'installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres du port. Reportez-vous aux instructions d'entretien de votre appareil.

- Depuis la page d'accueil de l'installateur d'appliance StorageGRID, sélectionnez **Démarrer l'installation**.

L'état actuel passe à « Installation en cours », et la page d'installation du moniteur s'affiche.



Si vous devez accéder manuellement à la page d'installation du moniteur, sélectionnez **Monitor installation** dans la barre de menu.

Surveillez l'installation de l'appliance de services StorageGRID

Le programme d'installation de l'appliance StorageGRID indique l'état jusqu'à ce que

l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appliance est redémarrée.

Étapes

- 1. Pour suivre la progression de l'installation, sélectionnez **Monitor installation** dans la barre de menu.

La page d'installation de Monitor affiche la progression de l'installation.

La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.



Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état « ignoré ».

- 2. Passez en revue l'état d'avancement des deux premières étapes d'installation.
 - **1. Configurer le stockage**

Au cours de cette étape, le programme d'installation efface toute configuration existante des disques et configure les paramètres hôte.
 - **2. Installez OS**

Au cours de cette étape, le programme d'installation copie l'image de base du système d'exploitation pour StorageGRID du nœud d'administration principal vers l'appliance ou installe le système d'exploitation de base à partir du package d'installation du nœud d'administration principal.
- 3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'un des événements suivants se produise :
 - Pour les nœuds de passerelle d'appliance ou les nœuds d'administration de l'appliance non primaire, l'étape **installer StorageGRID** s'interrompt et un message s'affiche sur la console intégrée, vous invitant à approuver ce nœud sur le nœud d'administration à l'aide du Gestionnaire de grille.
 - Pour les nœuds d'administration principaux de l'appliance, une cinquième phase (Load StorageGRID installer) s'affiche. Si la cinquième phase est en cours pendant plus de 10 minutes, actualisez la page manuellement.
- 4. Passez à l'étape suivante du processus de restauration pour le type de nœud de grille d'appliance que vous restaurez.

Type de restauration	Référence
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud d'administration non primaire	"Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire"
Nœud d'administration principal	"Configurez le nœud d'administration principal de remplacement"

Comment le support technique récupère un site StorageGRID

Si l'ensemble du site StorageGRID tombe en panne ou si plusieurs nœuds de stockage tombent en panne, vous devez contacter le support technique. Le support technique évalue votre situation, développe un plan de reprise, puis restaure les nœuds ou le site en panne en fonction des objectifs de votre entreprise, optimise le délai de restauration et évite les pertes de données inutiles.



La restauration du site ne peut être effectuée que par le support technique.

Les systèmes StorageGRID sont résilients pour de nombreuses défaillances et vous pouvez réaliser vous-même de nombreuses procédures de reprise et de maintenance. Cependant, il est difficile de créer une procédure simple et généralisée de récupération du site parce que les étapes détaillées dépendent de facteurs spécifiques à votre situation. Par exemple :

- **Vos objectifs d'entreprise**: Après la perte complète d'un site StorageGRID, vous devriez évaluer la meilleure façon d'atteindre vos objectifs d'entreprise. Par exemple, voulez-vous reconstruire le site perdu en place? Voulez-vous remplacer le site StorageGRID perdu à un nouvel emplacement ? La situation de chaque client est différente, et votre plan de reprise doit être conçu pour répondre à vos priorités.
- **Nature exacte de la défaillance** : avant de commencer une récupération de site, déterminez si des nœuds du site défaillant sont intacts ou si des nœuds de stockage contiennent des objets récupérables. Si vous reconstruisez des nœuds ou des volumes de stockage contenant des données valides, vous risquez de perdre des données superflues.
- **Règles ILM actives** : le nombre, le type et l'emplacement des copies d'objets de votre grille sont contrôlés par vos règles ILM actives. Les spécificités de vos règles ILM peuvent affecter la quantité de données récupérables, ainsi que les techniques de restauration spécifiques requises.



Si un site contient la seule copie d'un objet et que le site est perdu, l'objet est perdu.

- **Cohérence de compartiment (ou conteneur)** : la cohérence appliquée à un compartiment (ou conteneur) affecte si StorageGRID réplique entièrement les métadonnées d'objet sur tous les nœuds et sites avant de dire à un client que l'acquisition d'objet a réussi. Si la valeur de cohérence permet une cohérence éventuelle, certaines métadonnées d'objet peuvent avoir été perdues en cas de panne sur le site. Cela peut avoir un impact sur la quantité de données récupérables et éventuellement sur les détails de la procédure de restauration.
- **Historique des modifications récentes** : les détails de votre procédure de récupération peuvent être affectés par la présence ou non de procédures de maintenance en cours au moment de l'échec ou par la modification récente de vos politiques ILM. Le support technique doit évaluer l'historique récent de votre grille ainsi que sa situation actuelle avant de commencer une récupération de site.



La restauration du site ne peut être effectuée que par le support technique.

Il s'agit d'une présentation générale du processus utilisé par le support technique pour restaurer un site défaillant :

1. Support technique :
 - a. Effectue une évaluation détaillée de la défaillance.

- b. Travaillez avec vous pour examiner les objectifs de votre entreprise.
 - c. Développez un plan de reprise adapté à votre situation.
- 2. Si le nœud d'administration principal est défaillant, le support technique le récupère.
- 3. Support technique pour la restauration de tous les nœuds de stockage, voici les grandes lignes :
 - a. Remplacez le matériel ou les machines virtuelles du nœud de stockage selon les besoins.
 - b. Restaurez les métadonnées d'objet sur le site défaillant.
 - c. Restaurez les données d'objet vers les nœuds de stockage récupérés.



La perte de données se produit si les procédures de restauration d'un seul nœud de stockage défaillant sont utilisées.



Lorsqu'un site entier est en panne, le support technique utilise des commandes spécialisées pour restaurer avec succès les objets et les métadonnées d'objet.

- 4. Le support technique restaure les autres nœuds défaillants.

Une fois les métadonnées et les données d'objet restaurées, le support technique applique des procédures standard pour restaurer des nœuds de passerelle défaillants ou des nœuds d'administration non primaires.

Informations associées

["Mise hors service du site"](#)

Solutions et ressources StorageGRID

Aller à "[Solutions et ressources StorageGRID](#)" pour apprendre à tester et activer des applications dans votre environnement StorageGRID .

Comment gérer StorageGRID à l'aide de la console NetApp

Aller à "[Gestion de StorageGRID à l'aide de la console NetApp](#)" pour apprendre à gérer vos systèmes StorageGRID à partir de la console NetApp à l'aide de Grid Manager et à utiliser les services de données de la console NetApp pour les sauvegardes, la hiérarchisation des données, etc.

- BlueXP est désormais NetApp Console*

La console NetApp , construite sur la base BlueXP améliorée et restructurée, fournit une gestion centralisée du stockage NetApp et des services de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Pour plus de détails sur les changements, consultez le "[Notes de version de la console NetApp](#)".

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Licence API

Cette documentation n'octroie aucune licence ni aucun autre droit sur l'API REST StorageGRID S3. Toute utilisation ou tout accès à l'API REST StorageGRID S3 nécessite et est soumis à un accord de licence distinct avec NetApp.

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

https://library.netapp.com/ecm/ecm_download_file/ECMLP3373066

Informations sur le copyright

Copyright © 2026 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.