



Administrer le système

StorageGRID

NetApp
October 03, 2025

Sommaire

Administrer le système	1
Administrer StorageGRID	1
StorageGRID d'administration : présentation	1
Commencez avec StorageGRID	1
Contrôle de l'accès à StorageGRID	30
Gérer les paramètres de sécurité	80
Gérer les locataires	145
Configurez les connexions des clients S3 et Swift	167
Gestion des réseaux et des connexions	202
Utiliser AutoSupport	222
Gérer des nœuds de stockage	235
Gérer les nœuds d'administration	259
Gérer les nœuds d'archivage	281
Migrer les données vers StorageGRID	304
Gestion des objets avec ILM	306
Gérez les objets avec ILM : présentation	306
ILM et cycle de vie des objets	308
Définition d'une règle ILM	328
Définition d'une règle ILM	331
Créez des classes de stockage, des pools de stockage, des profils EC et des régions	335
Création d'une règle ILM	388
Création de la règle ILM	407
Utilisation des règles ILM et des règles ILM	431
Verrouillage des objets S3 avec ILM	436
Exemples de règles et de règles ILM	448
Durcissement du système	470
Durcissement du système : vue d'ensemble	470
Directives de renforcement des mises à niveau logicielles	470
Instructions de renforcement des réseaux StorageGRID	471
Instructions de renforcement pour les nœuds StorageGRID	473
Consignes de renforcement des certificats de serveur	476
Autres directives de durcissement	477
Configurez FabricPool	478
Configurer StorageGRID pour FabricPool : présentation	478
Association de StorageGRID en tant que Tier cloud	480
Utilisez la solution de gestion du cycle de vie des informations StorageGRID avec les données FabricPool	492
Créer une règle de classification du trafic pour FabricPool	495
Autres meilleures pratiques pour StorageGRID et FabricPool	498

Administrer le système

Administrer StorageGRID

StorageGRID d'administration : présentation

Suivez ces instructions pour configurer et administrer un système StorageGRID.

À propos de ces instructions

Ces instructions expliquent comment utiliser Grid Manager pour configurer des groupes et des utilisateurs, créer des comptes de locataires pour permettre aux applications client S3 et Swift de stocker et récupérer des objets, configurer et gérer des réseaux StorageGRID, configurer AutoSupport, gérer des paramètres de nœud, etc.

Ces instructions s'adresse au personnel technique qui devra configurer, administrer et prendre en charge un système StorageGRID après son installation.

Avant de commencer

- Vous disposez d'une compréhension générale du système StorageGRID.
- Vous disposez d'une connaissance assez détaillée des shells de commande Linux, de la mise en réseau et de la configuration matérielle du serveur.

Commencez avec StorageGRID

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94

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

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connectez-vous au Grid Manager

Vous accédez à la page de connexion de Grid Manager en entrant le nom de domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur Web pris en charge.

Ce dont vous avez besoin

- Vous disposez de vos identifiants de connexion.
- Vous avez l'URL pour Grid Manager.
- Vous utilisez un [navigateur web pris en charge](#).
- Les cookies sont activés dans votre navigateur Web.
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

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. Cependant, les nœuds d'administration ne sont pas exactement les mêmes :

- Les accusés de réception d'alarme (système hérité) effectués sur un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration. Pour cette raison, les informations affichées pour les alarmes peuvent ne pas être identiques sur chaque nœud d'administration.
- Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

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.

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL du Grid Manager :

```
https://FQDN_or_Admin_Node_IP/
```

où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe de nœuds d'administration haute disponibilité.

Si vous devez accéder à Grid Manager sur un port autre que le port standard pour HTTPS (443), entrez les informations suivantes, où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou une adresse IP et le port est le numéro de port :

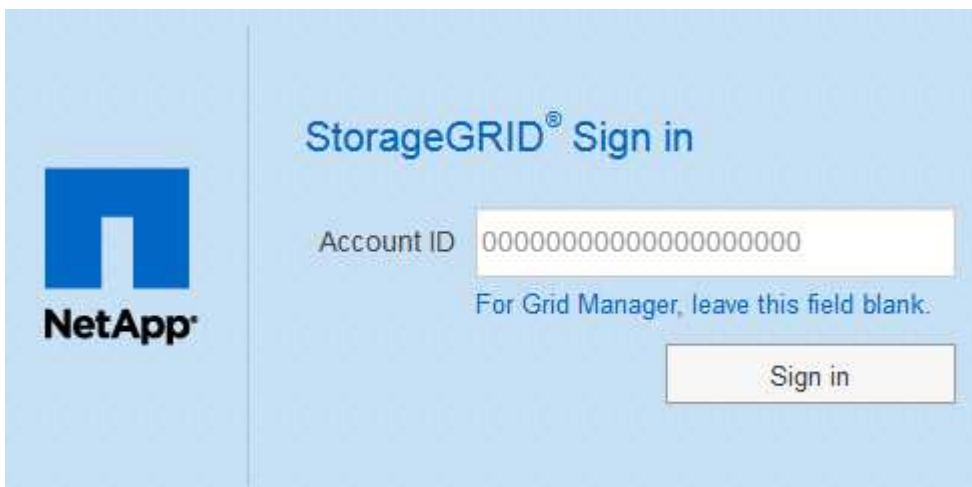
```
https://FQDN_or_Admin_Node_IP:port/
```

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 [À propos des certificats de sécurité](#)).
4. Connectez-vous au Grid Manager :

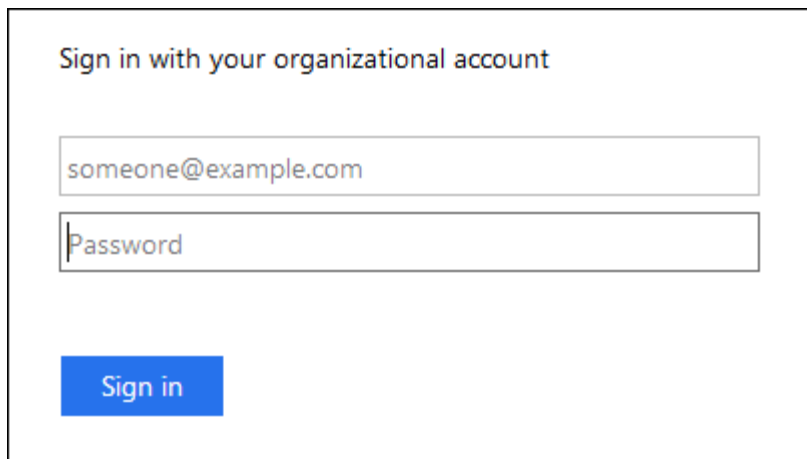
- Si l'authentification unique (SSO) n'est pas utilisée pour votre système StorageGRID :
 - i. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
 - ii. Sélectionnez **connexion**.

The image shows the 'StorageGRID® Grid Manager' login page. On the left is the NetApp logo. The main area has the title 'StorageGRID® Grid Manager'. Below it are two input fields: 'Username' and 'Password'. At the bottom right is a 'Sign in' button.

- Si l'authentification SSO est activée pour votre système StorageGRID et qu'il s'agit de la première fois que vous avez accédé à l'URL sur ce navigateur :
 - i. Sélectionnez **connexion**. Vous pouvez laisser le champ ID compte vide.

The image shows the 'StorageGRID® Sign in' page. On the left is the NetApp logo. The main area has the title 'StorageGRID® Sign in'. Below it is an 'Account ID' input field containing a long string of zeros. Below the field is the text 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.

- ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Par exemple :



Sign in with your organizational account

someone@example.com

Password

Sign in

- Si l'authentification SSO est activée pour votre système StorageGRID et que vous avez déjà accédé au Grid Manager ou à un compte de locataire :
 - i. Effectuez l'une des opérations suivantes :
 - Saisissez **0** (l'ID de compte pour le gestionnaire de grille) et sélectionnez **connexion**.
 - Sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents et sélectionnez **connexion**.



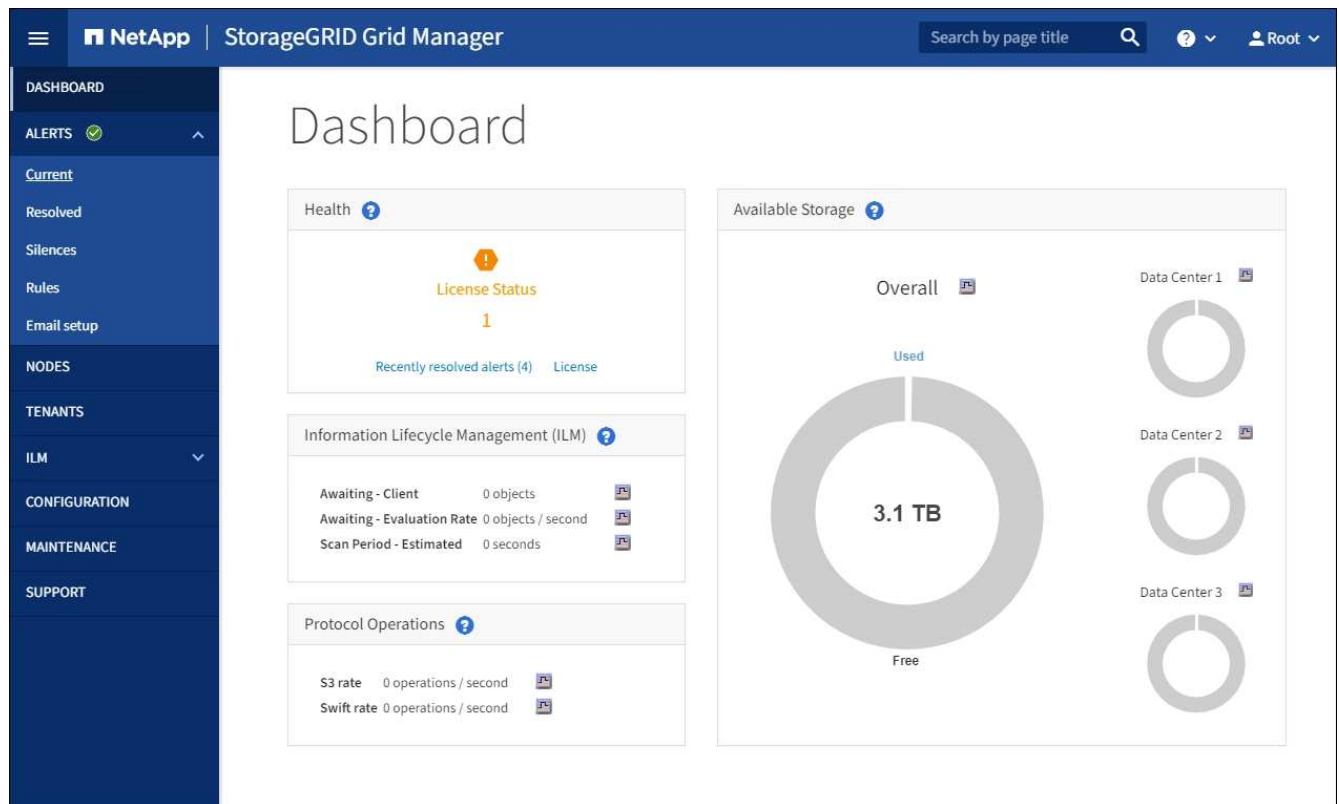
StorageGRID® Sign in

Recent Grid Manager

Account ID 0

Sign in

- ii. 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 de Grid Manager s'affiche, qui inclut le tableau de bord. Pour connaître les informations fournies, reportez-vous à la section [Afficher le tableau de bord](#).



5. Pour vous connecter à un autre nœud d'administration :

Option	Étapes
SSO non activé	- 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. - Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager. - Sélectionnez connexion.
SSO activé	Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Si vous vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter. Toutefois, si votre session SSO expire, vous êtes invité à saisir à nouveau vos informations d'identification. Remarque : SSO n'est pas disponible sur le port restreint Grid Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

- [Contrôle de l'accès par le biais de pare-feu](#)
- [Configurer l'authentification unique](#)

- Gérez les groupes d'administration
- Gérez les groupes haute disponibilité
- Utilisez un compte de locataire
- Surveiller et résoudre les problèmes

Déconnectez-vous du Grid Manager

Lorsque vous avez terminé de travailler avec le Gestionnaire de grille, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Sélectionnez votre nom d'utilisateur dans le coin supérieur droit.



2. Sélectionnez **Déconnexion**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. Remarque : si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous 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 SSO est activé et que vous êtes également connecté au Gestionnaire de tenant, vous devez également vous déconnecter du compte de tenant pour vous déconnecter de SSO.

Informations associées

- [Configurer l'authentification unique](#)
- [Utilisez un compte de locataire](#)

Changer votre mot de passe

Si vous êtes un utilisateur local de Grid Manager, vous pouvez modifier votre propre mot de passe.

Ce dont vous avez besoin

Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

Description de la tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans Grid Manager. 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**.

Modifiez le délai d'expiration de la session du navigateur

Vous pouvez contrôler si les utilisateurs de Grid Manager et de tenant Manager sont déconnectés s'ils sont inactifs pendant plus d'un certain temps.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Le délai d'inactivité de l'interface graphique est défini par défaut sur 900 secondes (15 minutes). Si la session de navigateur d'un utilisateur n'est pas active pendant cette période, la session est expirée.

Si nécessaire, vous pouvez augmenter ou diminuer le délai d'inactivité en définissant l'option d'affichage délai d'inactivité de l'interface graphique.

Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur est expirée, le système se comporte comme si l'utilisateur a sélectionné **Déconnexion** manuellement. L'utilisateur doit saisir à nouveau ses identifiants SSO pour accéder à StorageGRID. Voir [Configurer l'authentification unique](#).

Le délai d'expiration de session utilisateur peut également être contrôlé par les éléments suivants :



- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Par défaut, le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsqu'une authentification de l'utilisateur expire, cet utilisateur est automatiquement déconnecté, même si la valeur du délai d'inactivité de l'interface graphique n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai pour le fournisseur d'identité, en supposant que SSO est activé pour StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION système Options d'affichage**.
2. Pour **délai d'inactivité de l'interface graphique utilisateur**, entrez un délai d'expiration de 60 secondes ou plus.

Définissez ce champ sur 0 si vous ne souhaitez pas utiliser cette fonctionnalité. Les utilisateurs sont déconnectés 16 heures après leur connexion, quand leurs jetons d'authentification expirent.



Display Options

Updated: 2017-03-09 20:36:53 MST

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	☐

Apply Changes

3. Sélectionnez **appliquer les modifications**.

Le nouveau paramètre n'affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.

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.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

Description de la tâche

En cas de problème avec la licence logicielle de ce système StorageGRID, le panneau intégrité du tableau de bord inclut une icône d'état de la licence et un lien **Licence**. Le numéro indique le nombre de problèmes liés à la licence.



Étape

Pour afficher la licence, effectuez l'une des opérations suivantes :

- Dans le panneau Santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**. Ce lien apparaît uniquement en cas de problème avec la licence.
- Sélectionnez **MAINTENANCE système Licence**.

La page Licence s'affiche et fournit les informations suivantes en lecture seule sur la licence actuelle :

- ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
- Numéro de série de la licence
- Capacité de stockage sous licence de la grille
- Date de fin de la licence logicielle
- Date de fin du contrat de service de support
- Contenu du fichier texte de licence



Pour les licences émises avant StorageGRID 10.3, la capacité de stockage sous licence n'est pas incluse dans le fichier de licence et un message « Voir contrat de licence » s'affiche au lieu d'une valeur.

Mettez à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID à tout moment que les conditions de votre modification de licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez de la capacité de stockage supplémentaire pour votre grid.

Ce dont vous avez besoin

- Vous avez un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez la phrase secrète pour le provisionnement.

Étapes

1. Sélectionnez **MAINTENANCE système Licence**.
2. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.

3. Sélectionnez **Parcourir**.
4. Dans la boîte de dialogue Ouvrir, localisez et sélectionnez le nouveau fichier de licence (.txt) Et sélectionnez **Ouvrir**.

Le nouveau fichier de licence est validé et affiché.

5. Sélectionnez **Enregistrer**.

Utilisez l'API

Utilisez l'API de gestion du grid

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.

Ce dont vous avez besoin

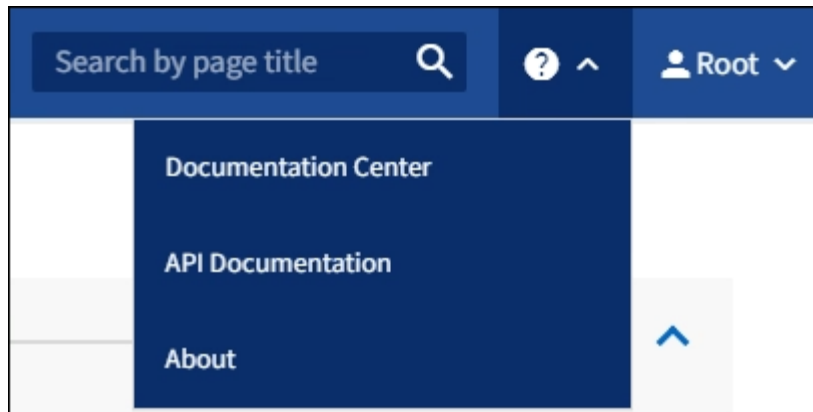
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.



Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Dans l'en-tête 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.

GET
/grid/groups
Lists Grid Administrator Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated — ▼
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	if set, the marker element is also returned — ▼
order string (query)	pagination order (desc requires marker) Available values : asc, desc — ▼

Responses
Response content type application/json ▼

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

- Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, 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**.
- Vérifiez le code de réponse pour déterminer si la demande a réussi.

L'API Grid Management organise les opérations disponibles dans les sections suivantes.



Cette liste inclut uniquement les opérations disponibles dans l'API publique.

- **Comptes** — opérations pour gérer les comptes de tenant du stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **Alarmes** — opérations pour répertorier les alarmes en cours (système hérité) et renvoyer des informations sur l'intégrité de la grille, y compris les alertes en cours et un résumé des États de connexion du nœud.
- **Alerte-historique** — opérations sur les alertes résolues.
- **Alertes-récepteurs** — opérations sur les récepteurs de notification d'alerte (e-mail).
- **Règles d'alerte** — opérations sur les règles d'alerte.
- **Seuils d'alerte** — opérations sur les silences d'alerte.
- **Alertes** — opérations sur les alertes.
- **Audit** — opérations pour répertorier et mettre à jour la configuration d'audit.
- **Auth** — opérations pour effectuer l'authentification de session utilisateur.

L'API Grid Management prend en charge le schéma d'authentification par jeton Bearer. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : porteur *token* »).



Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir « authentification dans l'API si l'authentification unique est activée ».

Voir « protection contre la contrefaçon de demandes intersites » pour des informations sur l'amélioration de la sécurité de l'authentification.

- **Certificats-client** — opérations pour 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 de gestion de grille. 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.
- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été désactivées.
- **dns-serveurs** — opérations pour répertorier et modifier les serveurs DNS externes configurés.
- **Endpoint-domain-names** — opérations pour lister et modifier les noms de domaine de nœud final.
- **Code d'effacement** — opérations sur les profils de code d'effacement.
- **Expansion** — opérations sur l'expansion (niveau procédure).
- **Nœuds d'extension** — opérations sur l'extension (au niveau du nœud).
- **Sites d'expansion** — opérations sur l'expansion (au niveau du site).
- **Grid-réseaux** — opérations pour lister et modifier la liste des réseaux de grille.
- **GRID-mots de passe** — opérations pour la gestion des mots de passe de grille.

- **Groupes** — opérations pour gérer les groupes d'administrateurs Grid locaux et pour extraire des groupes d'administrateurs Grid fédérés à partir d'un serveur LDAP externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** — opérations sur la gestion du cycle de vie de l'information (ILM).
- **Licence** — opérations pour récupérer et mettre à jour la licence StorageGRID.
- **Logs** — opérations de collecte et de téléchargement de fichiers journaux.
- **Métriques** — opérations sur les métriques StorageGRID incluant des requêtes métriques instantanées à un point unique dans les requêtes métriques de temps et de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.



Indicateurs qui incluent *private* dans leur nom sont destinés à un usage interne uniquement. Ces metrics sont susceptibles d'être modifiés sans préavis entre les versions d'StorageGRID.

- **Noeud-détails** — opérations sur noeud détails.
- **Node-Health** — opérations sur l'état de santé du noeud.
- **ntp-Server** — opérations pour répertorier ou mettre à jour les serveurs NTP (Network Time Protocol) externes.
- **Objets** — opérations sur les objets et les métadonnées d'objet.
- **Récupération** — opérations pour la procédure de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Régions** — opérations pour afficher et créer des régions.
- **s3-Object-lock** — opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-Certificate** — opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** — opérations sur la configuration SNMP actuelle.
- **Classes de trafic** — opérations pour les politiques de classification du trafic.
- **Réseau-client-non fiable** — opérations sur la configuration réseau client non fiable.
- **Utilisateurs** — opérations pour afficher et gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion du grid

L'API de gestion du grid utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La version majeure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées, qui sont **non compatibles** avec des versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées que **sont compatibles** avec des versions antérieures. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés. L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion de grille est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.



Vous pouvez utiliser l'API Grid Management pour configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section « config » de la documentation de l'API swagger. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients de l'API Grid Management pour utiliser la version la plus récente.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{IP-Address}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécifiez une version API pour une demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (/api/v3) ou un en-tête (Api-Version: 3). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez l' `csrfToken` paramètre à `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le `X-Csrf-Token` En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.



Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée

Utilisez l'API si l'authentification unique est activée (Active Directory)

Si vous l'avez [Authentification unique \(SSO\) configurée et activée](#) Et vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API tenant Management.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Ce dont vous avez besoin

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).
- Un exemple de flux de travail des requêtes Curl.

Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher :
`A valid SubjectConfirmation was not found on this Response.`



L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version.`

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
 - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
 - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` Passez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

- Méthode SSO. Entrez ADFS ou adfs.
- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé
- L'adresse de StorageGRID

- L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

- a. Déclarez les variables nécessaires pour la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

- b. Pour recevoir une URL d'authentification signée, lancez une demande POST à /api/v3/authorize-saml, Et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à `python -m json.tool` Pour supprimer l'encodage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
-H "accept: application/json" -H "Content-Type: application/json" \
--data '{"accountId": "$TENANTACCOUNTID"}' | python -m
json.tool
```

La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.


```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
  sSl%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Enregistrez le SAMLRequest à partir de la réponse pour une utilisation dans les commandes suivantes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Obtenir une URL complète incluant l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion à l'aide de l'URL de la réponse précédente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La réponse inclut l'ID de demande client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. Enregistrez l'ID de la demande client à partir de la réponse.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

- f. Envoyez vos informations d'identification à l'action de formulaire de la réponse précédente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$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=fZHRToMwFIZfhh...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Enregistrez le MSISAuth cookie de la réponse.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envoyez une demande GET à l'emplacement spécifié avec les cookies du POST d'authentification.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Les en-têtes de réponse contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse dans un champ de formulaire masqué.

```

HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XfXVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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. Enregistrez le SAMLResponse dans le champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

- j. À l'aide de la sauvegarde SAMLResponse, Faire un StorageGRID/api/saml-response Demande de génération d'un jeton d'authentification StorageGRID.

Pour RelayState, Utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API Grid Management.

```

curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool

```

La réponse inclut le jeton d'authentification.

```
{
  "apiVersion": "3.0",
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
  "responseTime": "2018-11-07T21:32:53.486Z",
  "status": "success"
}
```

- a. Enregistrez le jeton d'authentification dans la réponse sous MYTOKEN.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez maintenant utiliser MYTOKEN Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID simplement en vous connectant à partir de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, passez cookie "sso=true" Pour l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%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" Non fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A 204 No Content réponse indique que l'utilisateur est déconnecté.

```
HTTP/1.1 204 No Content
```

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous l'avez [Authentification unique \(SSO\) configurée et activée](#) Vous pouvez également utiliser Azure en tant que fournisseur SSO pour obtenir un jeton d'authentification valide pour l'API de gestion du grid ou l'API de gestion des locataires.

Connectez-vous à l'API si l'authentification unique Azure est activée

Ces instructions s'appliquent si vous utilisez Azure comme fournisseur d'identité SSO

Ce dont vous avez besoin

- Vous connaissez l'adresse e-mail SSO et le mot de passe d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` Script Python
- Le `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` script. Le script Python fait deux requêtes directement à StorageGRID (d'abord pour obtenir la SAMLRequest et plus tard pour obtenir le jeton d'autorisation), et appelle également le script Node.js pour interagir avec Azure afin d'effectuer les opérations SSO.

Les opérations SSO peuvent être exécutées à l'aide d'une série de requêtes d'API, mais cette opération n'est pas simple. Le module Puppeteer Node.js est utilisé pour gratter l'interface SSO Azure.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version.`

Étapes

1. Installez les dépendances requises comme suit :
 - a. Installez Node.js (voir "<https://nodejs.org/en/download/>").
 - b. Installez les modules Node.js requis (maripeteer et jsdom) :

```
npm install -g <module>
```

2. Passez le script Python à l'interpréteur Python pour exécuter le script.

Le script Python appelle ensuite le script Node.js correspondant pour exécuter les interactions SSO Azure.

3. Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
 - Adresse e-mail SSO utilisée pour se connecter à Azure
 - L'adresse de StorageGRID
 - L'ID du compte de locataire, pour accéder à l'API de gestion des locataires

4. Lorsque vous y êtes invité, saisissez le mot de passe et préparez-vous à fournir une autorisation MFA à Azure si nécessaire.

```
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 par message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

Utilisez l'API si l'authentification unique est activée (PingFederate)

Si vous l'avez [Authentification unique \(SSO\) configurée et activée](#) De plus, vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API tenant Management.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Ce dont vous avez besoin

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).
- Un exemple de flux de travail des requêtes Curl.

Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher :
A valid SubjectConfirmation was not found on this Response.



L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version.`

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
 - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
 - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` Passez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

- Méthode SSO. Vous pouvez entrer n'importe quelle variation de `""pingdén""` (PINGFEDERATE, pingfédéré, etc.).
- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou entrer n'importe quelle valeur.
- L'adresse de StorageGRID
- L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.
 - a. Déclarez les variables nécessaires pour la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

- b. Pour recevoir une URL d'authentification signée, lancez une demande POST à `/api/v3/authorize-saml`, Et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à `python -m json.tool` pour supprimer l'encodage

JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
-H "accept: application/json" -H "Content-Type: application/json" \
--data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Enregistrez le SAMLRequest à partir de la réponse pour une utilisation dans les commandes suivantes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Exportez la réponse et le cookie, et écho la réponse :

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

- e. Exporter la valeur 'pf.adapterId' et réafficher la réponse :

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

- f. Exporter la valeur « href » (supprimer la barre oblique inverse /) et afficher en écho la réponse :

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporter la valeur « action » :

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Envoyer des cookies avec des informations d'identification :

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Enregistrez le SAMLResponse dans le champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. À l'aide de la sauvegarde SAMLResponse, Faire un StorageGRID/api/saml-response Demande de génération d'un jeton d'authentification StorageGRID.

Pour RelayState, Utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool
```

La réponse inclut le jeton d'authentification.

```
{
  "apiVersion": "3.0",
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
  "responseTime": "2018-11-07T21:32:53.486Z",
  "status": "success"
}
```

- a. Enregistrez le jeton d'authentification dans la réponse sous MYTOKEN.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez maintenant utiliser MYTOKEN Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID simplement en vous connectant à partir de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, passez cookie "sso=true" Pour l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/ldap/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/ldap/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et redirectionner vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Supprimez le jeton de support StorageGRID.

La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si cookie "sso=true" Non fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A 204 No Content reponse indique que l'utilisateur est déconnecté.

```
HTTP/1.1 204 No Content
```

Contrôle de l'accès à StorageGRID

Modifiez la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète du provisionnement StorageGRID. La phrase de passe est requise pour les procédures de restauration, d'extension et de maintenance. La phrase de passe est également requise pour télécharger les sauvegardes du pack de récupération qui incluent les informations de topologie de la grille, les mots de passe de la console des nœuds grid et les clés de chiffrement pour le système StorageGRID.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.
- Vous disposez de la phrase secrète pour le provisionnement.

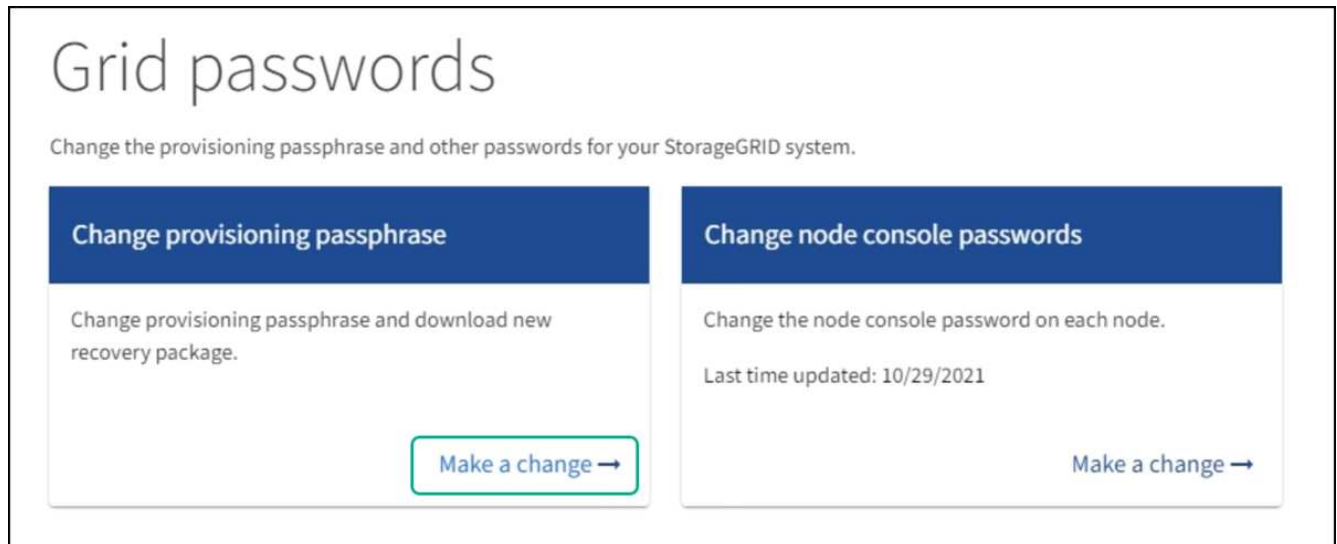
Description de la tâche

La phrase secrète de provisionnement est requise pour la plupart des procédures d'installation et de

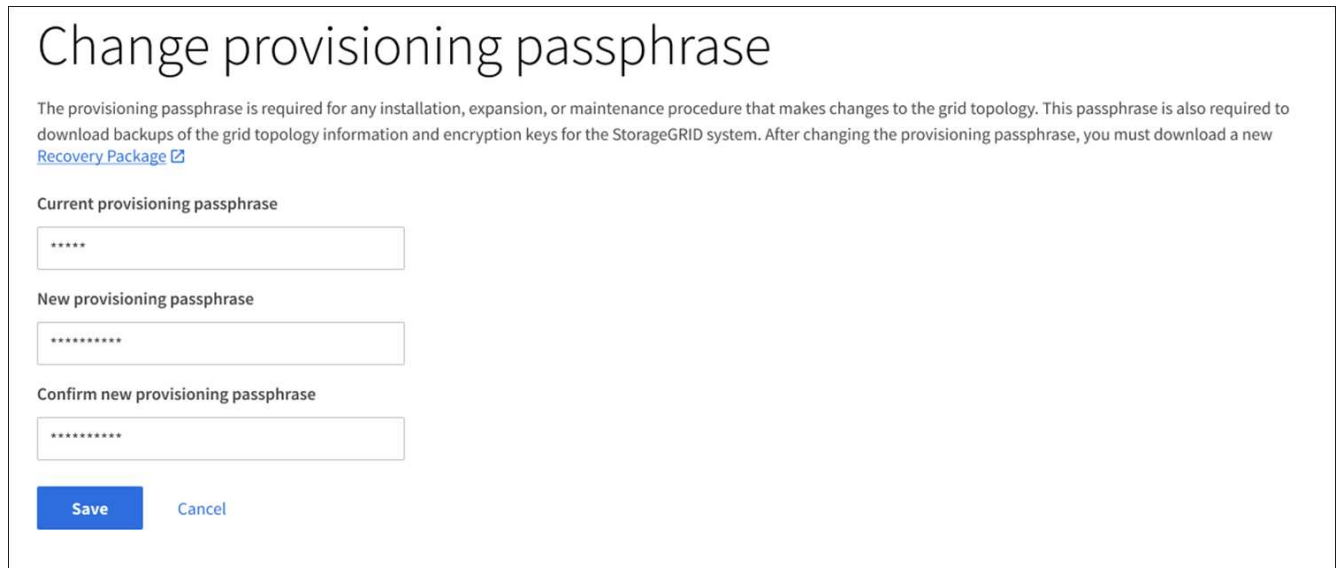
maintenance, et pour [Téléchargement du progiciel de restauration](#). La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier. Veuillez à documenter la phrase de passe de provisionnement et à la conserver dans un emplacement sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION** contrôle d'accès mots de passe de grille.



2. Sélectionnez **faire une modification** sous **Modifier la phrase de passe de provisionnement**.



3. Saisissez votre phrase secrète pour le provisionnement.
4. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases passe sont sensibles à la casse.
5. Stocker la nouvelle phrase secrète pour le provisionnement dans un emplacement sécurisé Elle est requise pour les procédures d'installation, d'extension et de maintenance.
6. Saisissez à nouveau la nouvelle phrase de passe et sélectionnez **Enregistrer**.

Le système affiche une bannière verte de réussite lorsque la modification de la phrase de passe de provisionnement est terminée.

Configuration > Grid passwords > Change provisioning passphrase

✔ **Success**
Provisioning passphrase changed successfully

Change provisioning passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to [download backups of the grid topology information and encryption keys for the StorageGRID system](#). After changing the provisioning passphrase, you must download a new [Recovery Package](#)

Current provisioning passphrase

New provisioning passphrase

Confirm new provisioning passphrase

7. Sélectionnez **progiciel de récupération**.

8. Entrez la nouvelle phrase de passe de provisionnement pour télécharger le nouveau progiciel de restauration.



Après avoir modifié la phrase de passe de provisionnement, vous devez télécharger immédiatement un nouveau progiciel de restauration. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grid dispose d'un mot de passe de console de nœud unique que vous devez vous connecter au nœud. Procédez comme suit pour modifier chaque mot de passe de console de nœud unique pour chaque nœud de votre grille.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur web pris en charge"](#).
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'administrateur à l'aide de SSH ou à l'utilisateur root via une connexion VM/console physique. Le processus de modification du mot de passe de la console de nœud crée de nouveaux mots de passe pour chaque nœud de votre grille et stocke les mots de passe dans une mise à jour `Passwords.txt` Fichier dans le progiciel de restauration. Les mots de passe sont répertoriés dans la colonne Mot de passe du `Passwords.txt` fichier.



Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Les mots de passe d'accès SSH ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** contrôle d'accès mots de passe de grille.
2. Sous **Modifier les mots de passe de la console de nœuds**, sélectionnez **faire une modification**.

Saisissez la phrase secrète pour le provisionnement

Étapes

1. Saisissez la phrase de passe de provisionnement pour votre grid.
2. Sélectionnez **Continuer**.

Téléchargez le progiciel de récupération actuel

Avant de modifier les mots de passe de la console de nœuds, téléchargez le progiciel de récupération actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de modification du mot de passe échoue pour un noeud quelconque.

Étapes

1. Sélectionnez **Télécharger le paquet de récupération**.
2. Copiez le fichier du progiciel de récupération (.zip) à deux emplacements sûrs, sécurisés et séparés.



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

3. Sélectionnez **Continuer**.
4. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à modifier les mots de passe de la console du nœud.

Vous ne pouvez pas annuler ce processus après son démarrage.

Changer les mots de passe de la console du nœud

Lorsque le processus de mot de passe de la console du nœud démarre, un nouveau package de récupération est généré, qui inclut les nouveaux mots de passe. Les mots de passe sont ensuite mis à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Sélectionnez **Télécharger nouveau paquet de récupération**.
3. Une fois le téléchargement terminé :
 - a. Ouvrez le .zip fichier.
 - b. Vérifiez que vous pouvez accéder au contenu, y compris au `Passwords.txt` qui contient les nouveaux mots de passe de la console du nœud.
 - c. Copiez le nouveau fichier de package de récupération (.zip) à deux emplacements sûrs, sécurisés et séparés.



N'écrasez pas l'ancien progiciel de récupération.

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.

4. Cochez la case pour indiquer que vous avez téléchargé le nouveau progiciel de restauration et vérifié le contenu.
5. Sélectionnez **Modifier les mots de passe de la console de nœuds** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cette opération peut prendre quelques minutes.

Si les mots de passe sont modifiés pour tous les nœuds, une bannière de réussite verte s'affiche. Passez à l'étape suivante.

En cas d'erreur lors du processus de mise à jour, un message de bannière indique le nombre de nœuds dont les mots de passe n'ont pas été modifiés. Le système réexécute automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine avec certains nœuds qui n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** s'affiche.

Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :

- a. Vérifiez les messages d'erreur répertoriés dans le tableau.
- b. Résolvez les problèmes.
- c. Sélectionnez **Réessayer**.



La tentative de nouveau modifie uniquement les mots de passe de la console de nœud sur les nœuds qui ont échoué lors des précédentes tentatives de changement de mot de passe.

6. Une fois que les mots de passe de la console du nœud ont été modifiés pour tous les nœuds, supprimez le [Premier package de récupération que vous avez téléchargé](#).
7. Vous pouvez également utiliser le lien **Recovery package** pour télécharger une copie supplémentaire du nouveau progiciel de récupération.

Contrôle de l'accès par le biais de pare-feu

Lorsque vous souhaitez contrôler l'accès par le biais de pare-feu, vous ouvrez ou fermez des ports spécifiques au niveau du pare-feu externe.

Contrôlez l'accès 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.

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 de l'API de gestion ne peuvent pas accéder à Grid Manager ou à l'API de gestion Grid. • 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](#)

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes et des utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification familières.

Configurer la fédération des identités pour Grid Manager

Vous pouvez configurer la fédération des identités dans Grid Manager si vous souhaitez que les groupes et les utilisateurs d'administration soient gérés dans un autre système, tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Instructions de configuration d'un serveur OpenLDAP](#).
- Si vous avez l'intention d'activer l'authentification unique (SSO), vous avez examiné le [conditions requises pour l'utilisation de l'authentification unique](#).
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identités utilise TLS 1.2 ou 1.3. Voir [Chiffrement pris en charge pour les connexions TLS sortantes](#).

Description de la tâche

Vous pouvez configurer un référentiel d'identité pour Grid Manager si vous souhaitez importer des groupes à partir d'un autre système, tel qu'Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administration. Les utilisateurs des groupes admin peuvent se connecter au gestionnaire de grille et effectuer des tâches en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre référentiel d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Gestionnaire de locataires et effectuer des tâches en fonction des autorisations attribuées au groupe dans le Gestionnaire de locataires. Voir [Créer un compte de locataire](#) et [Utilisez un compte de locataire](#) pour plus d'informations.

Entrez la configuration

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	Azure	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 utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
- **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
- **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
- **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.

- **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
- **Port** : port utilisé pour se connecter au serveur LDAP.



Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- `sAMAccountName` ou `uid`
- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
- **Azure** : `accountEnabled` et `userPrincipalName`
- **Mot de passe** : mot de passe associé au nom d'utilisateur.
- **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (`DC=storagegrid,DC=exemple,DC=com`) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.



Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

- **Format de nom d'utilisateur de liaison** (facultatif) : le modèle de nom d'utilisateur par défaut StorageGRID doit être utilisé si le motif ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

- **Modèle UserPrincipalName (Active Directory et Azure)** : `[USERNAME]@example.com`
- **Modèle de nom de connexion bas niveau (Active Directory et Azure)** : `example\[USERNAME]`
- **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=example,DC=com`

Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

- **Utilisez STARTTLS** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou autre, mais cette option n'est pas prise en charge pour Azure.
- **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.
- **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.



L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

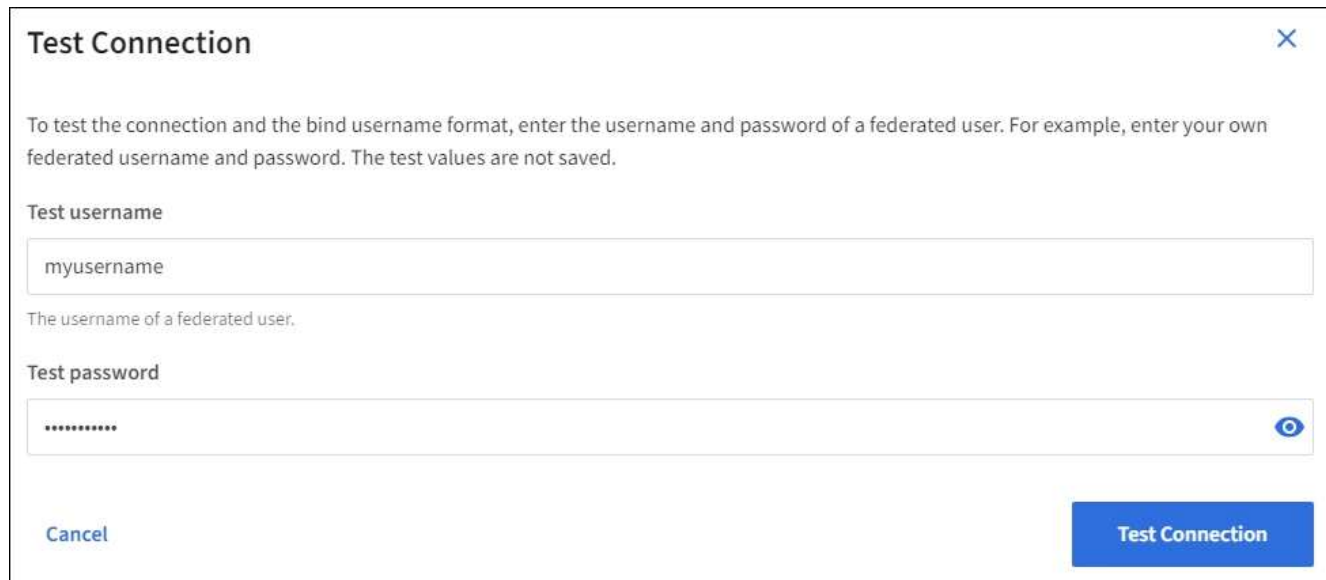
Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
 - Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Un message « Impossible d'établir la connexion test » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, comme @ ou /.



- Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.



L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si l'authentification unique (SSO) est définie sur **Enabled** ou **Sandbox mode**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir [Désactiver l'authentification unique](#).

Étapes

1. Accédez à la page fédération des identités.
2. Décochez la case **Activer la fédération d'identités**.

Instructions de configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les référentiels d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloque pas automatiquement l'accès S3 des utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez toute clé S3 pour l'utilisateur et 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 de l'adhésion au groupe inverse dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"].

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations relatives à la maintenance de l'adhésion au groupe inverse dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Gérez les groupes d'administration

Vous pouvez créer des groupes d'administration pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour pouvoir accéder au système StorageGRID.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Créer un groupe d'administration

Les groupes Admin vous permettent de déterminer quels utilisateurs peuvent accéder aux fonctions et opérations du gestionnaire de grille et de l'API Grid Management.

Accéder à l'assistant

1. Sélectionnez **CONFIGURATION** **contrôle d'accès groupes Admin**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs à partir du référentiel d'identité.

Groupe local

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d’affichage pour le groupe, que vous pourrez mettre à jour ultérieurement si nécessaire. Par exemple, « Maintenance Users » ou « ILM Administrators ».
3. Saisissez un nom unique pour le groupe, que vous ne pourrez pas mettre à jour ultérieurement.
4. Sélectionnez **Continuer**.

Groupe fédéré

1. Sélectionnez **Groupe fédéré**.
2. Entrez le nom du groupe à importer, exactement tel qu’il apparaît dans le référentiel d’identité configuré.
 - Pour Active Directory et Azure, utilisez sAMAccountName.
 - Pour OpenLDAP, utilisez le CN (Common Name).
 - Pour un autre LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

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 Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu’un groupe est défini sur **lecture seule**, l’utilisateur dispose d’un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs options [Autorisations de groupe](#).

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)

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

Si vous n’avez pas encore créé d’utilisateurs locaux, vous pouvez enregistrer le groupe sans ajouter d’utilisateurs. Vous pouvez ajouter ce groupe à l’utilisateur sur la page utilisateurs. Voir [Gérer les utilisateurs](#) pour plus d’informations.

2. Sélectionnez **Créer groupe** et **Terminer**.

Afficher et modifier les groupes d'administration

Vous pouvez afficher les détails des groupes existants, modifier un groupe ou dupliquer un groupe.

- Pour afficher les informations de base de tous les groupes, consultez le tableau de la page groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **actions** ou la page de détails.

Tâche	Menu actions	Page de détails
Afficher les détails du groupe	- Cochez la case correspondant au groupe. - Sélectionnez actions Afficher les détails du groupe.	Sélectionnez le nom du groupe dans le tableau.
Modifier le nom d'affichage (groupes locaux uniquement)	- Cochez la case correspondant au groupe. - Sélectionnez actions Modifier le nom du groupe. - Saisissez le nouveau nom. - Sélectionnez Enregistrer les modifications.	- Sélectionnez le nom du groupe pour afficher les détails. - Sélectionnez l'icône de modification . - Saisissez le nouveau nom. - Sélectionnez Enregistrer les modifications.
Modifier le mode d'accès ou les autorisations	- Cochez la case correspondant au groupe. - Sélectionnez actions Afficher les détails du groupe. - Si vous le souhaitez, modifiez le mode d'accès du groupe. - Sélectionner ou désélectionner les options éventuellement Autorisations de groupe. - Sélectionnez Enregistrer les modifications.	- Sélectionnez le nom du groupe pour afficher les détails. - Si vous le souhaitez, modifiez le mode d'accès du groupe. - Sélectionner ou désélectionner les options éventuellement Autorisations de groupe. - Sélectionnez Enregistrer les modifications.

Dupliquer un groupe

1. Cochez la case correspondant au 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.

1. Dans la page groupes, cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **actions Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations de groupe

Lors de la création de groupes d'utilisateurs admin, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctions spécifiques de Grid Manager. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administration pour déterminer les tâches que l'utilisateur peut effectuer.

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au Grid Manager ou à l'API Grid Management.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds
- Surveiller la topologie de la grille
- Afficher les alertes actuelles et résolues
- Afficher les alarmes actuelles et historiques (système hérité)
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher certaines informations sur les pages Configuration et maintenance

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre **mode d'accès** du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administration. Toute fonctionnalité qui n'est pas explicitement mentionnée requiert l'autorisation **accès racine**.

Accès racine

Cette autorisation donne accès à toutes les fonctions d'administration de la grille.

Accuser réception d'alarmes (existantes)

Cette autorisation permet d'accuser réception et de répondre aux alarmes (système hérité). Tous les utilisateurs connectés peuvent afficher les alarmes actuelles et historiques.

Si vous souhaitez qu'un utilisateur surveille la topologie de la grille et accuse réception des alarmes uniquement, vous devez attribuer cette autorisation.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **changer mot de passe root** de la page locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine local du locataire. Cette autorisation est également utilisée pour migrer les clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **changer mot de passe racine**.



Pour accorder l'accès à la page locataires, qui contient l'option **changer mot de passe racine**, attribuez également l'autorisation **comptes locataire**.

Configuration de la page de topologie grid

Cette autorisation permet d'accéder aux onglets Configuration de la page **SUPPORT Outils topologie de grille**.

ILM

Cette autorisation permet d'accéder aux options de menu **ILM** suivantes :

- Règles
- Stratégies
- Le code d'effacement
- Régions
- Pools de stockage



Les utilisateurs doivent disposer des autorisations **autre configuration de grille** et **Configuration de page de topologie de grille** pour gérer les classes de stockage.

Maintenance

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser les options suivantes :

- **CONFIGURATION contrôle d'accès:**
 - Mots de passe de grille
- **MAINTENANCE tâches:**
 - Désaffectation
 - De développement
 - Vérification de l'existence d'objet
 - Reprise après incident
- **MAINTENANCE système :**
 - Package de restauration
 - Mise à jour logicielle
- **SUPPORT Outils:**
 - Journaux

Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, ces

pages :

- **MAINTENANCE réseau:**
 - Serveurs DNS
 - Réseau Grid
 - Serveurs NTP
- **MAINTENANCE système :**
 - Licence
- **CONFIGURATION sécurité:**
 - Certificats
 - Noms de domaine
- **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 à la page **SUPPORT Outils métriques**. Cette autorisation permet également d'accéder à des requêtes de metrics Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management.

Recherche de métadonnées d'objet

Cette autorisation permet d'accéder à la page **ILM recherche de métadonnées objet**.

Autre configuration de grille

Cette autorisation donne accès à d'autres options de configuration de grille.



Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation **Grid topology page configuration**.

- **ILM :**
 - Niveaux de stockage
- **CONFIGURATION réseau :**
 - Coût des liens
- **CONFIGURATION système :**
 - Options d'affichage
 - Options de grid
 - Options de stockage
- **PRISE EN CHARGE alarmes (existantes) :**

- Événements personnalisés
- Alarmes globales
- Configuration de la messagerie existante

Administrateur de l'appliance de stockage

Cette autorisation permet d'accéder à la gamme E-Series SANtricity System Manager sur les appliances de stockage via Grid Manager.

Comptes de locataires

Cette autorisation donne accès à la page locataires, où vous pouvez créer, modifier et supprimer des comptes de tenant. Cette autorisation permet également aux utilisateurs d'afficher les stratégies de classification de trafic existantes.

Désactivez les fonctions à l'aide de l'API

Vous pouvez utiliser l'API de gestion de grille pour désactiver complètement certaines fonctions du système StorageGRID. Lorsqu'une fonction est désactivée, aucune autorisation ne peut être attribuée pour effectuer les tâches associées à cette fonctionnalité.

Description de la tâche

Le système de fonctions désactivées vous permet d'empêcher l'accès à certaines fonctions du système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur racine ou les utilisateurs appartenant à des groupes d'administration disposant de l'autorisation **accès racine** d'utiliser cette fonctionnalité.

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte le scénario suivant :

La Société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

*Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de grille. En désactivant complètement la fonction **Modifier le mot de passe racine du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A peut s'assurer qu'aucun utilisateur Admin, y compris l'utilisateur racine et les utilisateurs appartenant à des groupes avec l'autorisation **accès racine**, ne peut modifier le mot de passe de l'utilisateur racine d'un compte locataire.*

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management. Voir [Utilisez l'API de gestion du grid](#).
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour désactiver une fonction, par exemple changer le mot de passe racine du locataire, envoyez un corps à l'API comme suit :

```
{ "grid": {"changeTenantRootPassword": true} }
```

Une fois la demande terminée, la fonction de modification du mot de passe racine du locataire est

désactivée. L'autorisation de gestion **Modifier le mot de passe racine du locataire** n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire échouera avec ""403 interdit".

Réactiver les fonctions désactivées

Par défaut, vous pouvez utiliser l'API Grid Management pour réactiver une fonction qui a été désactivée. Toutefois, si vous souhaitez empêcher la réactivation des fonctions désactivées, vous pouvez désactiver la fonction **activeFeatures** elle-même.



La fonction **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonction, sachez que vous perdrez définitivement la capacité de réactiver les autres fonctions désactivées. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management.
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

```
{ "grid": null }
```

Lorsque cette demande est terminée, toutes les fonctions, y compris la fonction Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine** du locataire apparaît maintenant dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire va réussir, en supposant que l'utilisateur dispose de l'autorisation de gestion **accès racine** ou **changer le mot de passe racine du locataire**.



L'exemple précédent provoque la réactivation des fonctions *A// DESACTIVE*. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe racine du locataire et continuer à désactiver la fonction d'acquiescement d'alarme, envoyez cette demande PUT :

```
{ "grid": { "alarmAcknowledgment": true } }
```

Gérer les utilisateurs

Vous pouvez afficher les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Créez un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et attribuer chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer des utilisateurs et des groupes fédérés.

Le gestionnaire de grille 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

1. Sélectionnez **CONFIGURATION** **contrôle d'accès utilisateurs Admin**.
2. Sélectionnez **Créer utilisateur**.

Saisissez les informations d'identification de l'utilisateur

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

1. Vous pouvez éventuellement attribuer l'utilisateur à un ou plusieurs groupes pour déterminer les autorisations de l'utilisateur.

Si vous n'avez pas encore créé de groupes, vous pouvez enregistrer l'utilisateur sans sélectionner de groupes. Vous pouvez ajouter cet utilisateur à un groupe sur la page groupes.

Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir [Gérez les groupes d'administration](#) pour plus d'informations.

2. Sélectionnez **Créer utilisateur** et **Terminer**.

Afficher et modifier les utilisateurs locaux

Vous pouvez afficher les détails des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour modifier son nom complet, son mot de passe ou son appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au Grid Manager et à l'API Grid Management.

Vous ne pouvez modifier que les utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau de la page utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou modifier le mot de passe d'un utilisateur local, utilisez le menu **actions** ou la page de détails.

Toutes les modifications sont appliquées la prochaine fois que l'utilisateur se déconnecte, puis se reconnecte au Grid Manager.



Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **changer mot de passe** de la bannière du gestionnaire de grille.

Tâche	Menu actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case de l'utilisateur. b. Sélectionnez actions Afficher les détails de l'utilisateur.	Sélectionnez le nom de l'utilisateur dans le tableau.
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions Modifier le nom complet. c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer les modifications.
Refuser ou autoriser l'accès StorageGRID	a. Cochez la case de l'utilisateur. b. Sélectionnez actions Afficher les détails de l'utilisateur. c. Sélectionnez l'onglet accès. d. Sélectionnez Oui pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez non pour permettre à l'utilisateur de se connecter. e. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet accès. c. Sélectionnez Oui pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez non pour permettre à l'utilisateur de se connecter. d. Sélectionnez Enregistrer les modifications.
Modifier le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions Afficher les détails de l'utilisateur. c. Sélectionnez l'onglet Mot de passe. d. Saisissez un nouveau mot de passe. e. Sélectionnez Modifier le 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 Modifier le mot de passe.

Tâche	Menu actions	Page de détails
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez actions Afficher les détails de l'utilisateur . c. Sélectionnez l'onglet groupes. d. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. e. Sélectionnez Modifier les groupes pour sélectionner différents groupes. f. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet groupes. c. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. d. Sélectionnez Modifier les groupes pour sélectionner différents groupes. e. Sélectionnez Enregistrer les modifications .

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur avec les mêmes autorisations.

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 racine.

1. Sur la page utilisateurs, cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
2. Sélectionnez **actions Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utilisation de la connexion unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs n'ont accès qu'au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires si leurs identifiants sont autorisés à l'aide du processus de connexion SSO mis en œuvre par votre entreprise. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Fonctionnement de l'authentification unique

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language).

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque l'authentification SSO est activée.

Connectez-vous lorsque SSO est activé

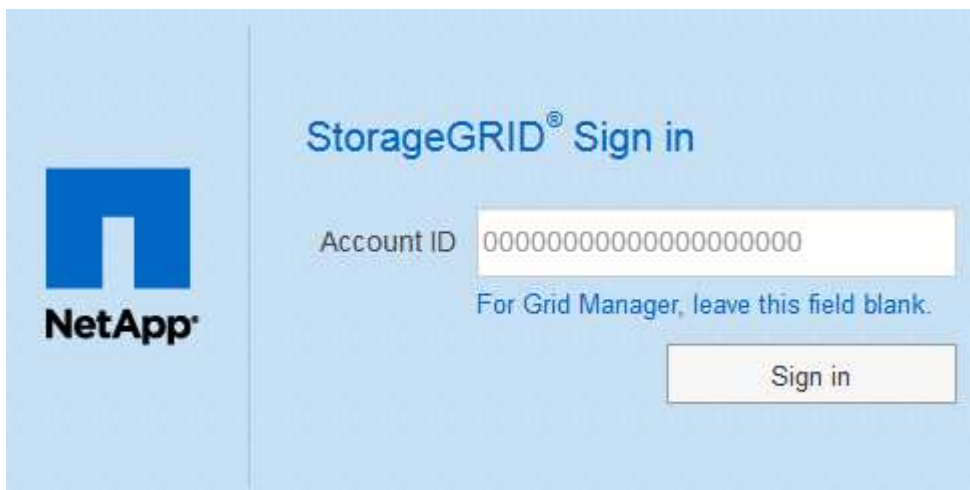
Lorsque l'authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

1. Entrez le nom de domaine complet ou l'adresse IP d'un nœud d'administration StorageGRID dans un navigateur Web.

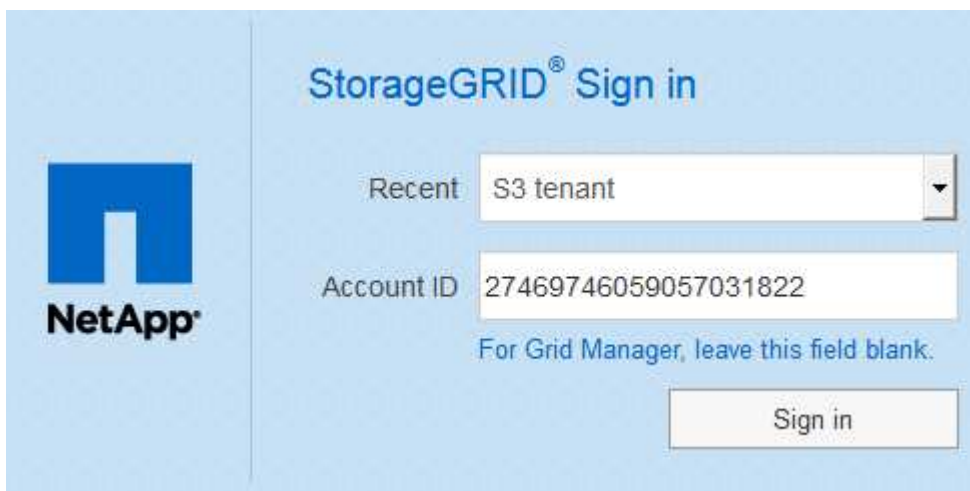
La page de connexion StorageGRID s'affiche.

- S'il s'agit de la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à entrer un ID de compte :



The image shows the 'StorageGRID® Sign in' page. On the left is the NetApp logo. The main area has the title 'StorageGRID® Sign in'. Below it is a text label 'Account ID' followed by a text input field containing a long string of zeros. Below the input field is the text 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.

- Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :



The image shows the 'StorageGRID® Sign in' page for a returning user. On the left is the NetApp logo. The main area has the title 'StorageGRID® Sign in'. Below it is a text label 'Recent' followed by a dropdown menu showing 'S3 tenant'. Below that is a text label 'Account ID' followed by a text input field containing the number '27469746059057031822'. Below the input field is the text 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.



La page de connexion StorageGRID n'apparaît pas lorsque vous saisissez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre entreprise, où vous pouvez [Connectez-vous à l'aide de vos identifiants SSO](#).

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :

- Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
- Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.

3. Sélectionnez **connexion**

StorageGRID vous redirige vers la page de connexion SSO de votre entreprise. Par exemple :

Sign in with your organizational account

someone@example.com

Password

Sign in

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 identifiants 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. Repérez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

La page de connexion StorageGRID s'affiche. La liste déroulante **comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder plus rapidement à ces interfaces utilisateur à l'avenir.

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration Remarque : si vous utilisez Azure pour SSO, la session de tous les nœuds d'administration peut prendre quelques minutes.
Gestionnaire de locataires sur un ou plusieurs nœuds d'administration	Gestionnaire de locataires sur n'importe quel nœud d'administration	Gestionnaire de locataires sur tous les nœuds d'administration
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.



Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Conditions requises pour l'utilisation de l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises dans cette section.

Exigences du fournisseur d'identités

StorageGRID prend en charge les fournisseurs d'identités SSO suivants :

- Service de fédération Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

Vous devez configurer la fédération des identités de votre système StorageGRID avant de pouvoir configurer

un fournisseur d'identités SSO. Le type de service LDAP que vous utilisez pour la fédération des identités contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Système de fichiers AD Windows Server 2022
- Système de fichiers AD Windows Server 2019
- Système de fichiers AD Windows Server 2016



Windows Server 2016 doit utiliser le "[Mise à jour KB3201845](#)", ou supérieur.

- AD FS 3.0, inclus avec la mise à jour Windows Server 2012 R2, ou une version ultérieure.

Supplémentaires requise

- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Configuration requise pour le certificat de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API de gestion du grid et à l'API de gestion des locataires. Lorsque vous configurez des approbations de tiers de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseur de services (PingFederate) pour StorageGRID, vous utilisez le certificat de serveur comme certificat de signature pour les requêtes StorageGRID.

Si ce n'est pas déjà fait [configuré un certificat personnalisé pour l'interface de gestion](#), vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID, les applications d'entreprise ou les connexions SP.



Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, d'une application d'entreprise ou d'un SP. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrices, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant à `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Configuration requise pour les ports

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique. Voir [Contrôle de l'accès par le biais de pare-feu](#).

Confirmez que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez déjà configuré la fédération des identités.

Étapes

1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.



Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

- a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
 - b. Sélectionnez **ACCESS MANAGEMENT identity federation**.
 - c. Confirmez que la case à cocher **Activer la fédération d'identités** n'est pas cochée.
 - d. Si c'est le cas, vérifiez que les groupes fédérés qui pourraient être utilisés pour ce compte de locataire ne sont plus nécessaires, désélectionnez la case à cocher et sélectionnez **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
 - a. Dans Grid Manager, sélectionnez **CONFIGURATION contrôle d'accès groupes d'administration**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation d'accès racine.
 - c. Se déconnecter.
 - d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
 3. S'il existe des comptes de tenant existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès racine peut se connecter :
 - a. Dans Grid Manager, sélectionnez **TENANTS**.
 - b. Sélectionnez le compte locataire, puis **actions Modifier**.
 - c. Dans l'onglet entrer les détails, sélectionnez **Continuer**.
 - d. Si la case à cocher **utiliser le propre référentiel d'identité** est sélectionnée, décochez la case et sélectionnez **Enregistrer**.

Edit the tenant

1 Enter details ————— 2 Select permissions

Select permissions

Select the permissions for this tenant account.

- ☐ Allow platform services ?
- ☐ Use own identity source ?
- ☐ Allow S3 Select ?

La page tenant s'affiche.

- Sélectionnez le compte de tenant, sélectionnez **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.
- Dans le Gestionnaire de locataires, sélectionnez **ACCESS MANAGEMENT Groups**.
- Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation d'accès racine pour ce locataire.
- Se déconnecter.
- Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

- [Conditions requises pour l'utilisation de l'authentification unique](#)
- [Gérez les groupes d'administration](#)
- [Utilisez un compte de locataire](#)

Utiliser le mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID. Une fois SSO activé, vous pouvez revenir en mode sandbox chaque fois que vous devez modifier ou tester à nouveau la configuration.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

- Vous avez configuré la fédération des identités pour votre système StorageGRID.
- Pour le type de service LDAP * de fédération d'identités, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous envisagez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. Le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour les demandes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Azure inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer en toute sécurité au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identités SSO pour créer une confiance de tiers de confiance (AD FS), une application d'entreprise (Azure) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer le SSO.

Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

1. Sélectionnez **CONFIGURATION** contrôle d'accès **Single Sign-on**.

La page connexion unique s'affiche, avec l'option **Disabled** sélectionnée.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Si les options d'état SSO ne s'affichent pas, confirmez que vous avez configuré le fournisseur d'identités en tant que référentiel d'identité fédéré. Voir [Conditions requises pour l'utilisation de l'authentification unique](#).

2. Sélectionnez **Sandbox mode**.

La section fournisseur d'identité s'affiche.

Saisissez les détails du fournisseur d'identité

1. Sélectionnez le **SSO type** dans la liste déroulante.
2. Renseignez les champs de la section Identity Provider en fonction du type SSO sélectionné.

Active Directory

1. Entrez le nom du service de fédération * pour le fournisseur d'identités, exactement comme il apparaît dans Active Directory Federation Service (AD FS).



Pour localiser le nom du service de fédération, accédez à Windows Server Manager. Sélectionnez **Outils AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

2. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

3. Dans la section partie de confiance, spécifiez l'identificateur de partie de confiance* pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque confiance de partie utilisatrices dans AD FS.

- Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prevoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez SG ou StorageGRID.
- Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identificateur. Par exemple : SG- [HOSTNAME]. Cette commande génère une table qui affiche l'identifiant de partie comptant pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

4. Sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.



Azure

1. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.

- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

2. Dans la section application entreprise, spécifiez le **Nom de l'application entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

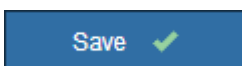
- Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prévoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez SG ou StorageGRID.
- Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identificateur. Par exemple : SG- [HOSTNAME] . Cela génère une table qui indique le nom d'une application d'entreprise pour chaque 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.

3. Suivez les étapes de la section [Création d'applications d'entreprise dans Azure AD](#) Pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.
4. Depuis Azure AD, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ URL* des métadonnées de fédération correspondant dans StorageGRID.
5. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.



PingFederate

1. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.
 - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
 - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

2. Dans la section SP (Service Provider), spécifiez l'ID de connexion **SP** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.

- Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prévoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
- Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Ce tableau génère un ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.



Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID. La présence d'une connexion SP pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

3. Spécifiez l'URL des métadonnées de fédération pour chaque 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>
```

4. Sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.



Configurez les approbations des parties utilisatrices, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox s'affiche. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions de présentation.

StorageGRID peut rester en mode sandbox tant que nécessaire. Toutefois, lorsque **Sandbox mode** est sélectionné sur la page connexion unique, SSO est désactivé pour tous les utilisateurs StorageGRID. Seuls les utilisateurs locaux peuvent se connecter.

Procédez comme suit pour configurer les approbations de tiers de confiance (Active Directory), les applications d'entreprise complètes (Azure) ou les connexions SP (PingFederate).

Active Directory

1. Accédez à Active Directory Federation Services (AD FS).
2. Créez une ou plusieurs fiducies de tiers de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page authentification unique StorageGRID.

Vous devez créer une confiance pour chaque nœud d'administration indiqué dans le tableau.

Pour obtenir des instructions, reportez-vous à la section [Créer des fiducies de tiers de confiance dans AD FS](#).

Azure

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 Single Sign-on**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes de la section [Création d'applications d'entreprise dans Azure AD](#) Pour charger le fichier de métadonnées SAML de chaque nœud d'administration dans l'application d'entreprise Azure correspondante.

PingFederate

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 Single Sign-on**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. [Créez une ou plusieurs connexions de fournisseur de services pour StorageGRID](#). Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué dans le tableau de la page d'authentification unique StorageGRID) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

Vous devez créer une connexion SP pour chaque nœud d'administration affiché dans le tableau.

Tester les connexions SSO

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID, vous devez confirmer que l'authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d'administration.

Active Directory

1. Sur la page d'ouverture de session unique de StorageGRID, localisez le lien dans le message en mode Sandbox.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.

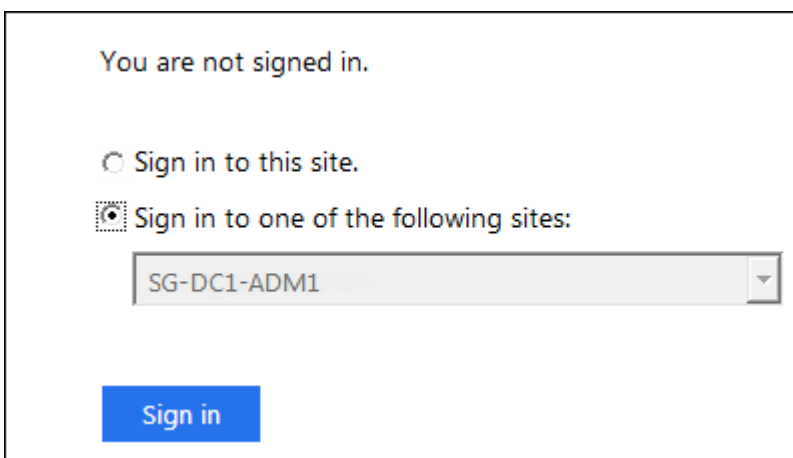
Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/dfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Sélectionnez le lien ou copiez-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.

✓ Single sign-on authentication and logout test completed successfully.

- Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Azure

1. Accédez à la page d'identification unique sur le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.

✓ Single sign-on authentication and logout test completed successfully.

- Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

1. Sur la page d'ouverture de session unique de StorageGRID, sélectionnez le premier lien dans le message en mode Sandbox.

Sélectionnez et testez un lien à la fois.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.

✓ Single sign-on authentication and logout test completed successfully.

- Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
3. Cliquez sur le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si un message page expirée s'affiche, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activez l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser la fonctionnalité SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer cette fonctionnalité pour l'ensemble du système StorageGRID.



Lorsque l'authentification SSO est activée, tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

1. Sélectionnez **CONFIGURATION** **contrôle d'accès Single Sign-on**.
2. Définissez l'état SSO sur **activé**.
3. Sélectionnez **Enregistrer**.
4. Vérifiez le message d'avertissement et sélectionnez **OK**.

L'authentification unique est désormais activée.



Si vous utilisez le portail Azure et que vous accédez à StorageGRID à partir du même ordinateur que celui que vous utilisez pour accéder à Azure, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (utilisateur d'un groupe fédéré importé dans StorageGRID) Ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des fiducies de tiers de confiance dans AD FS

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer une confiance de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations tierces via les commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou en saisissant manuellement les données.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **AD FS** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir [Utiliser le mode sandbox](#).
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie comptant pour chaque nœud d'administration de votre système. Ces valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.
- Si vous créez manuellement la confiance de la partie utilisatrices, vous disposez du certificat personnalisé

chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.

Description de la tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Créez une confiance en vous appuyant sur Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties qui font confiance.

Étapes

1. Dans le menu Démarrer de Windows, sélectionnez l'icône PowerShell avec le bouton droit de la souris et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, saisissez la commande suivante :

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Pour *Admin_Node_Identifier*, Entrez l'identifiant de partie de confiance du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : SG-DC1-ADM1.
- Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils AD FS Management**.

L'outil de gestion AD FS s'affiche.

4. Sélectionnez **AD FS fiducies de partie de confiance**.

La liste des fiducies de tiers de confiance s'affiche.

5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
 - a. Recherchez la confiance de la partie de confiance que vous venez de créer.
 - b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
 - c. Sélectionnez une stratégie de contrôle d'accès.
 - d. Sélectionnez **appliquer**, puis **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte comptant :
 - a. Recherchez la confiance de la partie de confiance que vous venez de créer.
 - b. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
 - c. Sélectionnez **Ajouter règle**.
 - d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.

e. Sur la page configurer la règle, entrez un nom d’affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.

f. Pour le magasin d’attributs, sélectionnez **Active Directory**.

g. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

i. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, confirmez que l’adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.

8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d’administration de votre système StorageGRID.

9. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu’elles sont correctement configurées. Voir [Utiliser le mode Sandbox](#) pour obtenir des instructions.

Créez une confiance de partie de confiance en vous important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque confiance de fournisseur en accédant aux métadonnées SAML de chaque nœud d’administration.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.

2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.

3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.

4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.

5. Dans **adresse de métadonnées de fédération (nom d’hôte ou URL)**, saisissez l’emplacement des métadonnées SAML pour ce nœud d’administration :

`https://Admin_Node_FQDN/api/saml-metadata`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du même nœud d’administration. (Si nécessaire, vous pouvez utiliser l’adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

6. Terminez l’assistant confiance de la partie de confiance, enregistrez la confiance de la partie de confiance et fermez l’assistant.



Lors de la saisie du nom d’affichage, utilisez l’identificateur de partie comptant pour le noeud d’administration, exactement comme il apparaît sur la page d’ouverture de session unique dans le Gestionnaire de grille. Par exemple : SG-DC1-ADM1.

7. Ajouter une règle de sinistre :

- a. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d’émission des sinistres**.
- b. Sélectionnez **Ajouter règle** :
- c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
- d. Sur la page configurer la règle, entrez un nom d’affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.

- e. Pour le magasin d’attributs, sélectionnez **Active Directory**.
- f. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
- g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
- h. Sélectionnez **Terminer** et sélectionnez **OK**.

8. Confirmez que les métadonnées ont été importées avec succès.

- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
- b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, confirmez que l’adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d’administration de votre système StorageGRID.

10. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu’elles sont correctement configurées. Voir [Utiliser le mode Sandbox](#) pour obtenir des instructions.

Créer une confiance de partie de confiance manuellement

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement** et sélectionnez **Suivant**.
5. Suivez l’assistant confiance de la partie de confiance :
 - a. Entrez un nom d’affichage pour ce nœud d’administration.

Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple : SG-DC1-ADM1.

- b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.
- c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.
- d. Saisissez l'URL du nœud final du service SAML pour le nœud d'administration :

`https://Admin_Node_FQDN/api/saml-response`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. 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 nœud d'administration :

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, Entrez l'identifiant de partie de confiance du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : SG-DC1-ADM1.

- f. Vérifiez les paramètres, enregistrez la confiance de la partie utilisatrices et fermez l'assistant.

La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.



Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

- 6. Pour démarrer l'assistant règle de sinistre, sélectionnez **Ajouter règle** :
 - a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
 - b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.
 - c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - d. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
 - e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
 - f. Sélectionnez **Terminer** et sélectionnez **OK**.
- 7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
- 8. Dans l'onglet **Endpoints**, configurez le nœud 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 nœud d'administration :

`https://Admin_Node_FQDN/api/saml-logout`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

- a. Sélectionnez **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :

- a. Ajouter le certificat personnalisé :

- Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
- Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` Répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.

Remarque : utilisation du certificat par défaut du nœud d'administration (`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

- b. Sélectionnez **appliquer**, puis **OK**.

Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir [Utiliser le mode sandbox](#) pour obtenir des instructions.

Création d'applications d'entreprise dans Azure AD

Vous utilisez Azure AD pour créer une application d'entreprise pour chaque nœud d'administration de votre système.

Ce dont vous avez besoin

- Vous avez commencé à configurer la connexion unique pour StorageGRID et vous avez sélectionné **Azure** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir [Utiliser le mode sandbox](#).
- Vous disposez du **Nom d'application entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID.



Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Azure Active Directory.
- Vous disposez d'un compte Azure avec un abonnement actif.
- Vous avez l'un des rôles suivants dans le compte Azure : administrateur global, administrateur des applications clouds, administrateur d'applications clouds ou propriétaire du principal du service.

Accéder à Azure AD

1. Connectez-vous au "[Portail Azure](#)".
2. Accédez à "[Azure Active Directory](#)".
3. Sélectionnez "[Les applications d'entreprise](#)".

Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Azure dans StorageGRID, vous devez utiliser Azure pour créer une application d'entreprise pour chaque nœud d'administration. Vous allez copier les URL de métadonnées de la fédération à partir d'Azure et les coller dans les champs URL* de métadonnées de la fédération correspondants sur la page d'ouverture de session unique de StorageGRID.

1. Répétez les étapes suivantes pour chaque nœud d'administration.
 - a. Dans le volet applications Azure Enterprise, sélectionnez **Nouvelle application**.
 - b. Sélectionnez **Créez votre propre application**.
 - c. Pour le nom, entrez le **nom de l'application entreprise** que vous avez copié à partir du tableau Détails du nœud d'administration sur la page connexion unique StorageGRID.
 - d. Laissez le bouton radio **intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie)** sélectionné.
 - e. Sélectionnez **Créer**.
 - f. Sélectionnez le lien **Get Started** dans **2. Configurez la case Single Sign On** ou sélectionnez le lien **Single Sign-on** dans la marge de gauche.
 - g. Sélectionnez la case **SAML**.
 - h. Copiez l'URL **App Federation Metadata URL**, que vous trouverez sous **étape 3 SAML Signing Certificate**.
 - i. Accédez à la page d'ouverture de session unique StorageGRID et collez l'URL dans le champ **URL de métadonnées de fédération** qui correspond au nom de l'application **entreprise** que vous avez utilisée.
2. Une fois que vous avez collé une URL de métadonnées de fédération pour chaque nœud d'administration et apporté toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page d'ouverture de session unique StorageGRID.

Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID.

Répétez cette procédure pour chaque nœud d'administration :

1. Connectez-vous à StorageGRID à partir du nœud d'administration.
2. Sélectionnez **CONFIGURATION contrôle d'accès Single Sign-on**.
3. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
4. Enregistrez le fichier que vous allez télécharger dans Azure AD.

Téléchargez les métadonnées SAML sur chaque application d'entreprise

Après le téléchargement d'un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID, effectuez les opérations suivantes dans Azure AD :

1. Revenez au portail Azure.
2. Répétez cette procédure pour chaque application d'entreprise :



Vous devrez peut-être actualiser la page applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

- a. Accédez à la page Propriétés de l'application d'entreprise.
 - b. Définissez **affectation requise** sur **non** (sauf si vous souhaitez configurer séparément les affectations).
 - c. Accédez à la page Single Sign-on.
 - d. Terminez la configuration SAML.
 - e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.
 - f. Une fois le fichier chargé, sélectionnez **Enregistrer**, puis **X** pour fermer le volet. Vous revenez à la page configurer un Single Sign-on avec SAML.
3. Suivez les étapes de la section [Utiliser le mode sandbox](#) pour tester chaque application.

Créer des connexions de fournisseur de services (SP) dans PingFederate

Vous utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration de votre système. Pour accélérer le processus, vous importez les métadonnées SAML à partir de StorageGRID.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **Ping Federate** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir [Utiliser le mode sandbox](#).
- Vous disposez de l'ID de connexion * SP* pour chaque nœud d'administration de votre système. Ces valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.
- Vous 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 <https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html> ["Guide de

référence de l'administrateur"] Pour PingFederate Server. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.

- Vous disposez de l'autorisation Admin pour PingFederate Server.

Description de la tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées sur votre version.

Remplir les conditions préalables dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lors de la configuration des connexions du processeur de service.

Créer un magasin de données

Si ce n'est pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lorsque [configuration de la fédération des identités](#) À StorageGRID.

- **Type:** Répertoire (LDAP)
- **Type LDAP :** Active Directory
- **Nom d'attribut binaire :** saisissez **objectGUID** dans l'onglet attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

- **Type:** LDAP Nom d'utilisateur Mot de passe validateur des informations d'identification
- **Magasin de données :** sélectionnez le magasin de données que vous avez créé.
- **Base de recherche :** saisissez des informations à partir de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche :** sAMAccountName=\${username}
- **Portée :** sous-arbre

Créer une instance d'adaptateur IDP

Si ce n'est déjà fait, créez une instance de carte IDP.

1. Accédez à **Authentication Integration IDP Adapters**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IDP adapter**.
4. Dans l'onglet carte IDP, sélectionnez **Ajouter une nouvelle ligne à 'Validators Credentials'**.
5. Sélectionner [validateur des informations d'identification du mot de passe](#) vous avez créé.
6. Dans l'onglet attributs de l'adaptateur, sélectionnez l'attribut **nom d'utilisateur** pour **pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

1. Allez à **sécurité certificats de clés de déchiffrement de signature**.
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, passez à [Créer des connexions SP supplémentaires](#) pour créer des connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

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

1. Dans l'onglet Importer les métadonnées, sélectionnez **fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page d'authentification unique StorageGRID pour le nœud d'administration.
3. Passez en revue le résumé des métadonnées et les informations de l'onglet informations 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

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

1. Dans l'onglet mappage de la source d'authentification, sélectionnez **mappage d'une nouvelle instance de carte**.
2. Dans l'onglet instance de la carte, sélectionnez **instance d'adaptateur** vous avez créé.
3. Dans l'onglet méthode de mappage, sélectionnez **recupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet User Lookup Source d'attribut, sélectionnez **Add Attribute Source**.
5. Dans l'onglet magasin de données, fournissez une description et sélectionnez **magasin de données** que vous avez ajouté.
6. Dans l'onglet LDAP Directory Search :
 - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
 - Pour l'étendue de la recherche, sélectionnez **sous-arbre**.
 - Pour la classe d'objet racine, recherchez l'attribut **objectGUID** et ajoutez-le.
7. Dans l'onglet types d'encodage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet filtre LDAP, entrez **sAMAccountName=\${username}**.
9. Dans l'onglet attribut Contract Expédié par contrat, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** dans la liste déroulante valeur.
10. Vérifiez et enregistrez la source d'attribut.
11. Dans l'onglet Source de l'attribut FailSave, sélectionnez **abandonner la transaction SSO**.
12. Passez en revue le résumé et sélectionnez **Done**.
13. Sélectionnez **Done**.

Configurer les paramètres de protocole

1. Dans l'onglet **connexion SP Browser SSO Paramètres de protocole**, sélectionnez **configurer les paramètres de protocole**.
2. Dans l'onglet URL du service client assertion, acceptez les valeurs par défaut qui ont été importées à partir des métadonnées SAML StorageGRID (**POST** pour la liaison et `/api/saml-response` Pour l'URL du point final).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut qui ont été importées à partir des métadonnées StorageGRID SAML (**REDIRECT** pour la liaison et `/api/saml-logout` Pour l'URL du point final).
4. Dans l'onglet liaisons SAML autorisées, désélectionnez **ARTEFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases à cocher **exiger la signature des demandes d'autorisation** et **toujours signer l'assertion** sélectionnées.
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

1. Dans l'onglet connexion SP, sélectionnez **informations d'identification**.
2. Dans l'onglet informations d'identification, sélectionnez **configurer les informations d'identification**.
3. Sélectionner [signature du certificat](#) vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **gérer les paramètres de vérification de signature**.
 - a. Dans l'onglet modèle de confiance, sélectionnez **non ancré**.
 - b. Dans l'onglet certificat de vérification de signature, vérifiez les informations de certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Passez en revue les écrans de résumé et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion du processeur de service pour créer les connexions du processeur de service dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.



Les connexions SP des différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de signature, Et l'URL de réponse SLO.

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 le contrat d'attribut de création d'assertion**.
 - c. Supprimez l'entrée pour **urn:oid**.
 - d. Sélectionnez **Enregistrer**.

Désactiver l'authentification unique

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération des identités.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

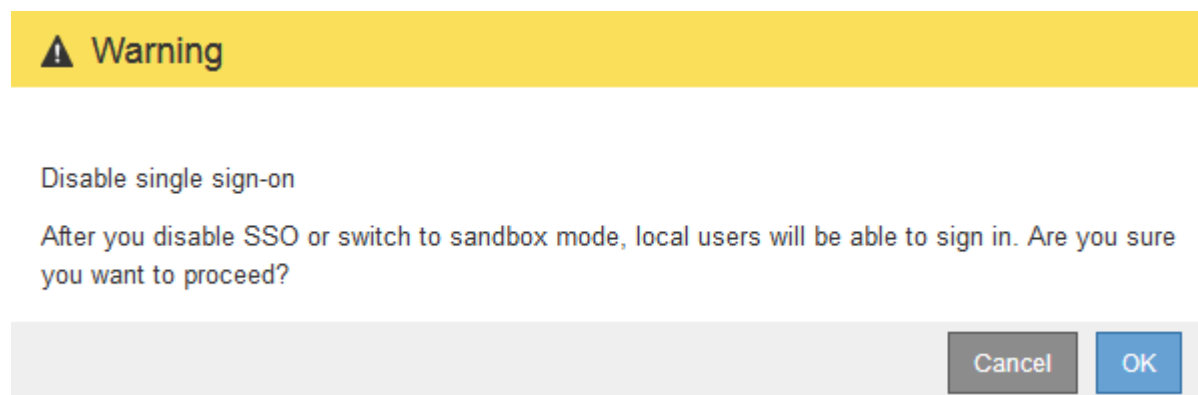
Étapes

1. Sélectionnez **CONFIGURATION** **contrôle d'accès Single Sign-on**.

La page authentification unique s'affiche.

2. Sélectionnez l'option **Disabled**.
3. Sélectionnez **Enregistrer**.

Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.



4. Sélectionnez **OK**.

La prochaine fois que vous vous connectez à StorageGRID, la page de connexion StorageGRID s'affiche et vous devez entrer le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique pour un nœud d'administration

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez le mot de passe de l'utilisateur racine local.

Description de la tâche

Après avoir désactivé SSO pour un 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 à cocher **Activer SSO** sur la page d'ouverture de session unique dans Grid Manager reste sélectionnée et tous les paramètres SSO existants sont conservés à moins que vous ne les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :

- a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Exécutez la commande suivante : `disable-saml`

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver l'authentification SSO.

Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

La page de connexion à Grid Manager s'affiche car SSO a été désactivé.

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.

6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :

- a. Sélectionnez **CONFIGURATION contrôle d'accès Single Sign-on**.
- 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 **Déconnexion** et fermez le gestionnaire de grille.
- c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :
 - Exécutez la commande suivante : `enable-saml`

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

Confirmez que vous souhaitez activer le SSO.

Un message indique que l'authentification unique est activée sur le nœud.

- Redémarrez le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Gérer les paramètres de sécurité

Gérer les certificats

À propos des certificats de sécurité

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur 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 cryptent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

StorageGRID inclut une autorité de certification intégrée qui génère un certificat d'autorité de certification interne Grid lors de l'installation du système. Par défaut, le certificat de l'autorité de certification Grid est utilisé pour sécuriser le trafic StorageGRID interne. Une autorité de certification externe peut émettre des certificats personnalisés qui sont entièrement conformes aux politiques de sécurité des informations de votre entreprise. Bien que vous puissiez utiliser le certificat d'autorité de certification Grid pour un environnement non productif, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions du serveur.
- Tous les certificats personnalisés doivent être conformes au [directives de renforcement du système](#) pour les certificats de serveur.
- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé 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.

1. Dans 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).

GlobalGrid CAClientLoad balancer endpointsTenantsOther

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 ne pouvez accéder à un onglet que si vous disposez de l'autorisation appropriée.
 - **Global** : sécurise l'accès à StorageGRID à partir de navigateurs Web et de clients API externes.
 - **Grid CA** : sécurise le trafic StorageGRID interne.
 - **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
 - **Points d'extrémité de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et Swift et l'équilibreur de charge StorageGRID.
 - **Locataires** : sécurise les connexions aux serveurs de fédération d'identités ou des terminaux de service de plate-forme aux ressources de stockage S3.
 - **Autre** : sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

Chaque onglet est décrit ci-dessous avec des liens vers des détails de certificat supplémentaires.

Mondial

Les certificats globaux sécurisent l'accès StorageGRID à partir de navigateurs Web et de clients API S3 et Swift externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- [Certificat de l'interface de gestion](#): Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID.
- [Certificat API S3 et Swift](#): Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 et Swift utilisent pour télécharger et télécharger les données d'objet.

Les informations sur les certificats globaux installés comprennent :

- **Nom** : nom du certificat avec lien vers la gestion du certificat.
- **Description**
- **Type** : personnalisé ou par défaut. + vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité de la grille.
- **Date d'expiration** : si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
 - [Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID](#) Utilisé pour les connexions Grid Manager et tenant Manager.
 - [Remplacez le certificat API S3 et Swift](#) Utilisé pour les connexions nœud de stockage, service CLB (obsolète) et point final de l'équilibreur de charge (facultatif).
- [Restaurez le certificat de l'interface de gestion par défaut.](#)
- [Restaurez le certificat API S3 et Swift par défaut.](#)
- [Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé.](#)
- Copiez ou téléchargez le [certificat de l'interface de gestion](#) ou [Certificat API S3 et Swift](#).

CA grille

Le [Certificat CA de la grille](#), Généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic StorageGRID interne.

Les informations sur le certificat comprennent la date d'expiration du certificat et son contenu.

C'est possible [Copiez ou téléchargez le certificat de l'autorité de certification Grid](#), mais vous ne pouvez pas le changer.

Client

[Certificats client](#), Généré par une autorité de certification externe, sécurisez les connexions entre les outils de contrôle externes et la base de données StorageGRID Prometheus.

La table de certificats possède une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que la date d'expiration du certificat.

Vous pouvez :

- [Téléchargez ou générez un nouveau certificat client.](#)
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
 - [Modifiez le nom du certificat client.](#)
 - [Définissez l'autorisation d'accès Prometheus.](#)
 - [Téléchargez et remplacez le certificat client.](#)
 - [Copiez ou téléchargez le certificat client.](#)
 - [Supprimez le certificat client.](#)
- Sélectionnez **actions** pour accélérer [modifier](#), [attacher](#), ou [déposer](#) un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions Supprimer**.

Terminaux d'équilibrage de charge

[Certificats de noeud final de l'équilibreur de charge](#), Que vous téléchargez ou générez, sécurisez les connexions entre les clients S3 et Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des noeuds finaux de l'équilibreur de charge comporte une ligne pour chaque noeud final de l'équilibreur de charge configuré et indique si le certificat API S3 et Swift global ou un certificat de point final d'équilibreur de charge personnalisé est utilisé pour le noeud final. La date d'expiration de chaque certificat s'affiche également.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Vous pouvez :

- [Sélectionnez un nom de noeud final pour ouvrir un onglet de navigateur contenant des informations sur le noeud final de l'équilibreur de charge, y compris ses détails de certificat.](#)
- [Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool.](#)
- [Utilisez le certificat global d'API S3 et Swift](#) au lieu de générer un nouveau certificat de terminal de l'équilibreur de charge.

Locataires

Les locataires peuvent utiliser [certificats de serveur de fédération des identités](#) ou [certificats de terminal du service de plate-forme](#) Pour sécuriser leurs connexions avec StorageGRID.

La table de tenant dispose d'une ligne pour chaque locataire et indique si chaque locataire a l'autorisation d'utiliser ses propres services de référentiel d'identité ou de plate-forme.

Vous pouvez :

- [Sélectionnez un nom de locataire pour vous connecter au Gestionnaire de tenant](#)
- [Sélectionnez un nom de locataire pour afficher les détails de la fédération des identités du locataire](#)
- [Sélectionnez un nom de locataire pour afficher les détails des services de plateforme du locataire](#)
- [Spécifiez un certificat de noeud final du service de plate-forme pendant la création du noeud final](#)

Autre

StorageGRID utilise d'autres certificats de sécurité pour des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. Voici d'autres certificats de sécurité :

- [Certificats de fédération des identités](#)
- [Certificats de pool de stockage cloud](#)
- [Certificats de serveur de gestion des clés \(KMS\)](#)
- [Certificats d'authentification unique](#)
- [Certificats de notification d'alerte par e-mail](#)
- [Certificats de serveur syslog externe](#)

Informations indique le type de certificat utilisé par une fonction et ses dates d'expiration de certificat de serveur et de client, le cas échéant. La sélection d'un nom de fonction ouvre un onglet de navigateur dans lequel vous pouvez afficher et modifier les détails du certificat.



Vous ne pouvez afficher et accéder aux informations d'autres certificats que si vous disposez de l'autorisation appropriée.

Vous pouvez :

- [Afficher et modifier un certificat de fédération d'identités](#)
- [Télécharger les certificats du serveur de gestion des clés \(KMS\) et du client](#)
- [Spécification d'un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure](#)
- [Spécifiez manuellement un certificat SSO pour la confiance de la partie utilisatrices](#)
- [Spécifiez un certificat pour les notifications par e-mail d'alerte](#)
- [Spécifiez un certificat de serveur syslog externe](#)

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers des articles contenant des instructions de mise en œuvre.

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	CONFIGURATION sécurité certificats , sélectionnez l'onglet Global , puis certificat d'interface de gestion	Configurer les certificats d'interface de gestion

Certificat API S3 et Swift

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 ou Swift sécurisées vers un nœud de stockage, vers le service CLB (Connection Load Balancer) obsolète sur un nœud de passerelle et les terminaux de l'équilibreur de charge (facultatif).	CONFIGURATION sécurité certificats , sélectionnez l'onglet Global , puis S3 et Swift API certificates	Configurez les certificats API S3 et Swift

Certificat CA de la grille

Voir la [Description du certificat CA de la grille par défaut](#).

Certificat du client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes.	CONFIGURATION sécurité certificats, puis sélectionnez l'onglet client	Configurer les certificats client

Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un 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 de Global Certificat API S3 et Swift Certificat permettant d'authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, il n'est pas nécessaire 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 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 des identités	Utiliser la fédération des identités

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 STOCKAGE (S3) noeuds finaux des services de plate-forme	Créer un terminal de services de plate-forme Modifier le point final des services de plate-forme

Certificat de terminal Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion à partir d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob Storage. Un certificat différent est requis pour chaque type de fournisseur cloud.	ILM pools de stockage	Création d'un pool de stockage cloud

Certificat de 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 SSO (Single Sign-on)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identités, tels que Active Directory Federation Services (AD FS) et StorageGRID utilisés pour les demandes SSO (Single Sign-on).	CONFIGURATION contrôle d'accès Single Sign-on	Configurer l'authentification unique

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.	ALERTE Configuration de la messagerie	Configurez les notifications par e-mail pour les alertes

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui consigne les événements dans StorageGRID. Remarque : un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	CONFIGURATION surveillance serveur d'audit et syslog , puis sélectionnez configurer serveur syslog externe	Configurer un serveur syslog externe

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.

2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : serveur de gestion externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Configurer les certificats de serveur

Types de certificat de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (algorithme de signature numérique de courbe elliptique).

Pour plus d'informations sur la sécurisation des connexions clients par StorageGRID pour l'API REST, reportez-vous à la section [Utilisation de S3](#) ou [Utiliser Swift](#).

Configurer les certificats d'interface de gestion

Vous pouvez remplacer le certificat de l'interface de gestion par défaut par un certificat personnalisé unique qui permet aux utilisateurs d'accéder à Grid Manager et au Gestionnaire de locataires sans rencontrer d'avertissement de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

Description de la tâche

Par défaut, chaque nœud d'administration est doté d'un certificat signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commun et une clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients

doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au tenant Manager. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, en fonction de l'autorité de certification racine (AC) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification Grid dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Gestionnaire de locataires.



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en consultant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.



Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous [restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée](#).

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (.key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

Générez un certificat

Générez les fichiers de certificat du serveur.



La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisée signé par une autorité de certification externe.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

- **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés 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.
- **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides**: Nombre de jours après la création que le certificat expire.

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.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.

Description de la tâche

La meilleure pratique pour un environnement de production consiste à utiliser un certificat signé par une autorité de certification externe.

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Pour `--domains`, Utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple : `*.ui.storagegrid.example.com` utilise le caractère générique `*` pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com`.
- Réglez `--type` à `management` Pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.
- Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.



La période de validité d'un certificat commence quand `make-certificate` est exécuté. Vous devez vous assurer que le client de gestion est synchronisé avec la même source horaire que StorageGRID ; sinon, le client peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

Le résultat contient le certificat public requis par votre client de l'API de gestion.

4. Sélectionnez et copiez le certificat.

Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`
6. Vérifiez que le certificat a été configuré :
 - a. Accédez au Grid Manager.
 - b. Sélectionnez **CONFIGURATION sécurité certificats**

- c. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat de l'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA .pem fichier. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Configurez les certificats API S3 et Swift

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 ou Swift vers les nœuds de stockage, le service CLB (Connection Load Balancer) obsolète sur les nœuds de passerelle ou pour charger les nœuds finaux de l'équilibreur. Le certificat de serveur personnalisé de remplacement est spécifique à votre

organisation.

Description de la tâche

Par défaut, chaque nœud de stockage est doté d'un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au 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 également installer le certificat d'autorité de certification Grid dans le client API S3 ou Swift que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration du certificat de serveur global pour S3 et l'API Swift** est déclenchée lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher quand le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en regardant la date d'expiration du certificat API S3 et Swift dans l'onglet Global.

Vous pouvez charger ou générer un certificat API S3 et Swift personnalisé.

Ajoutez un certificat S3 et Swift personnalisé

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (.key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de délivrance de certificat intermédiaire. Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM pour chaque certificat API S3 et Swift personnalisé chargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

- **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés 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.
- **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides**: Nombre de jours après la création que le certificat expire.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et PEM pour le certificat d'API S3 et Swift personnalisé qui a été généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, un certificat signé par l'autorité de certification qui a été chargé ou un certificat personnalisé qui a été généré.



Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.
7. Après avoir ajouté un certificat d'API S3 et Swift personnalisé, la page de certificats d'API S3 et Swift affiche des informations détaillées sur le certificat d'API S3 et Swift personnalisé utilisé. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat API S3 et Swift par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 et Swift par défaut pour les connexions des clients S3 et Swift vers les nœuds de stockage et du service CLB obsolète sur les nœuds de passerelle. Cependant, vous ne pouvez pas utiliser le certificat API S3 et Swift par défaut pour un nœud final d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat par défaut**.

Lorsque vous restaurez la version par défaut du certificat de l'API globale S3 et Swift, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 et Swift par défaut sera utilisé pour les nouvelles connexions clients S3 et Swift ultérieures aux nœuds de stockage et pour le service CLB obsolète sur les nœuds de passerelle.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 et Swift par défaut.

Si vous disposez de l'autorisation d'accès racine et que le certificat d'API S3 et Swift personnalisé a été utilisé pour les connexions de terminal de l'équilibreur de charge, une liste de terminaux d'équilibreur de charge qui ne seront plus accessibles via le certificat d'API S3 et Swift par défaut s'affiche. Accédez à [Configurer les terminaux de l'équilibreur de charge](#) pour modifier ou supprimer les points finaux affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Téléchargez ou copiez le certificat API S3 et Swift

Vous pouvez enregistrer ou copier le contenu du certificat de l'API S3 et Swift pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA .pem fichier. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Informations associées

- [Utilisation de S3](#)
- [Utiliser Swift](#)
- [Configurez les noms de domaine de terminaux API S3](#)

Copiez le certificat de l'autorité de certification Grid

StorageGRID utilise une autorité de certification interne pour sécuriser le trafic interne, Ce certificat ne change pas si vous téléchargez vos propres certificats.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si un certificat de serveur personnalisé a été configuré, les applications client doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat de l'autorité de certification depuis le système StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificate PEM**, téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat .pem fichier.

- a. Sélectionnez **Télécharger le certificat**.
- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Copier le certificat PEM**.
- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et qui ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP utilisant FabricPool, vous pouvez générer ou charger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées

parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, reportez-vous à la section [Configuration de StorageGRID pour FabricPool](#).



Le service distinct Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète et n'est pas recommandé pour une utilisation avec 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 nœud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA facultatif.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.



Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.

Configurer les certificats client

Les certificats client permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, ce qui fournit un moyen sécurisé aux outils externes de surveillance StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations de certificat dans l'outil externe.

Voir les informations sur [utilisation du certificat de sécurité général](#) et [configuration des certificats de serveur personnalisés](#).



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en consultant la date d'expiration du certificat client dans l'onglet client.



Si vous utilisez un serveur de gestion des clés (KMS) pour protéger les données sur les nœuds d'appliance spécialement configurés, consultez les informations spécifiques à propos de [Téléchargement d'un certificat client KMS](#).

Ce dont vous avez besoin

- Vous disposez de l'autorisation d'accès racine.

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Pour configurer un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
 - Si vous avez configuré le certificat de l'interface de gestion StorageGRID, l'autorité de certification, le certificat client et la clé privée sont utilisés pour configurer le certificat de l'interface de gestion.
 - Pour télécharger votre propre certificat, la clé privée du certificat est disponible sur votre ordinateur local.
 - La clé privée doit avoir été enregistrée ou enregistrée au moment de sa création. Si vous ne disposez pas de la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
 - Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Suivez la procédure de votre scénario pour ajouter un certificat client :

- [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. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Dans la section **Type de certificat**, téléchargez le certificat de l'interface de gestion **.pem** fichier.
 - a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
 - b. Téléchargez 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.

6. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

- a. **Nom** : saisissez un nom pour la connexion.

StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

- c. Activez **TLS client Auth** et **avec CA Cert**.

- d. Sous TLS/SSL Auth Details, copiez et collez :

- Le certificat CA de l'interface de gestion à **CA Cert**
- Le certificat client à **Cert client**
- La clé privée pour **clé client**

- e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

- f. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section [Instructions de surveillance de StorageGRID](#).

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. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Dans la section **Type de certificat**, téléchargez le certificat client, la clé privée et le bundle CA .pem fichiers :
 - a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
 - b. Téléchargez des fichiers de certificat client, de clé privée et 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.

7. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

- a. **Nom** : saisissez un nom pour la connexion.

StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

- c. Activez **TLS client Auth** et avec **CA Cert**.

- d. Sous TLS/SSL Auth Details, copiez et collez :

- Le certificat CA de l'interface de gestion à **CA Cert**
- Le certificat client à **Cert client**
- La clé privée pour **clé client**

- e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

- f. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section [Instructions de surveillance de StorageGRID](#).

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. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.

4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Dans la section **Type de certificat**, sélectionnez **générer certificat**.
6. Spécifiez les informations de certificat :
 - **Nom de domaine** : un ou plusieurs noms de domaine complets du noeud d'administration à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
 - **IP** : une ou plusieurs adresses IP de noeud d'administration à inclure dans le certificat.
 - **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
7. Sélectionnez **generate**.
8. 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.

9. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

10. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **Global**.
11. Sélectionnez **certificat d'interface de gestion**.
12. Sélectionnez **utiliser le certificat personnalisé**.
13. Téléchargez les fichiers Certificate.pem et private_key.pem à partir du [détails du certificat client](#) étape. Il n'est pas nécessaire de télécharger le pack CA.
 - a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
 - b. Téléchargez chaque fichier de certificat (`.pem`).
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

14. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.
 - a. **Nom** : saisissez un nom pour la connexion.

StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

- c. Activez **TLS client Auth** et avec **CA Cert**.

- d. Sous TLS/SSL Auth Details, copiez et collez :

- Le certificat client de l'interface de gestion à la fois **CA Cert** et **client Cert**
- 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.

- f. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section [Instructions de surveillance de StorageGRID](#).

Modifier les certificats client

Vous pouvez modifier un certificat de client d'administrateur pour changer son nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**
4. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
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 :
 - **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés 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.
 - **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
 - **Jours valides**: Nombre de jours après la création que le certificat expire.

- c. Sélectionnez **generate**.

- d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.



Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

Téléchargez ou copiez les certificats client

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

- a. Sélectionnez **Télécharger le certificat**.
- b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

Copier le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Copier le certificat PEM**.
- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats client

Si vous n'avez plus besoin d'un certificat de client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat à supprimer.

3. Sélectionnez **Supprimer**, puis confirmez.



Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet client, puis sélectionnez **actions Supprimer**.

Après la suppression d'un certificat, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les serveurs de gestion des clés

Configurer les serveurs de gestion des clés : présentation

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés (KMS) afin de protéger les données sur les nœuds d'appliance spécialement configurés.

Qu'est-ce qu'un serveur de gestion des clés (KMS) ?

Un serveur de gestion des clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance à moins que le nœud ne puisse 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.

Étudiez les méthodes de cryptage StorageGRID

StorageGRID fournit 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 configurez un serveur de gestion des clés pour le site StorageGRID (CONFIGURATION sécurité serveur de gestion des clés) et activez le cryptage des noeuds 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.  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.
Sécurité des disques dans SANtricity System Manager	Si la fonction sécurité des disques est activée pour une appliance de stockage, 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.	Appliances de stockage dotées de disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Ne peut pas être utilisé avec certains dispositifs de stockage ni avec des appliances de service. • Dispositifs de stockage SG6000 • Appliances de stockage SG5700 • Appliances de stockage SG5600
Option de grille de chiffrement d'objet stocké	L'option Inenregistré Object Encryption peut être activée dans Grid Manager (CONFIGURATION System Grid options). Lorsqu'il est activé, tout nouvel objet qui n'est pas chiffré au niveau du compartiment ou au niveau de l'objet est chiffré lors de l'ingestion.	Ingestion récente des données d'objet S3 et Swift. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. • Configurez le chiffrement des objets stockés

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement de compartiment S3	Vous émettez une demande de chiffrement Put bucket pour activer le chiffrement du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. • Utilisation de S3
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une demande S3 pour stocker un objet et inclure le <code>x-amz-server-side-encryption</code> en-tête de demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. • Utilisation de S3
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. • <code>x-amz-server-side-encryption-customer-algorithm</code> • <code>x-amz-server-side-encryption-customer-key</code> • <code>x-amz-server-side-encryption-customer-key-MD5</code>	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. • Utilisation de S3
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.

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. • "Amazon simple Storage Service - Guide des développeurs : protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement à la fois. Par exemple :

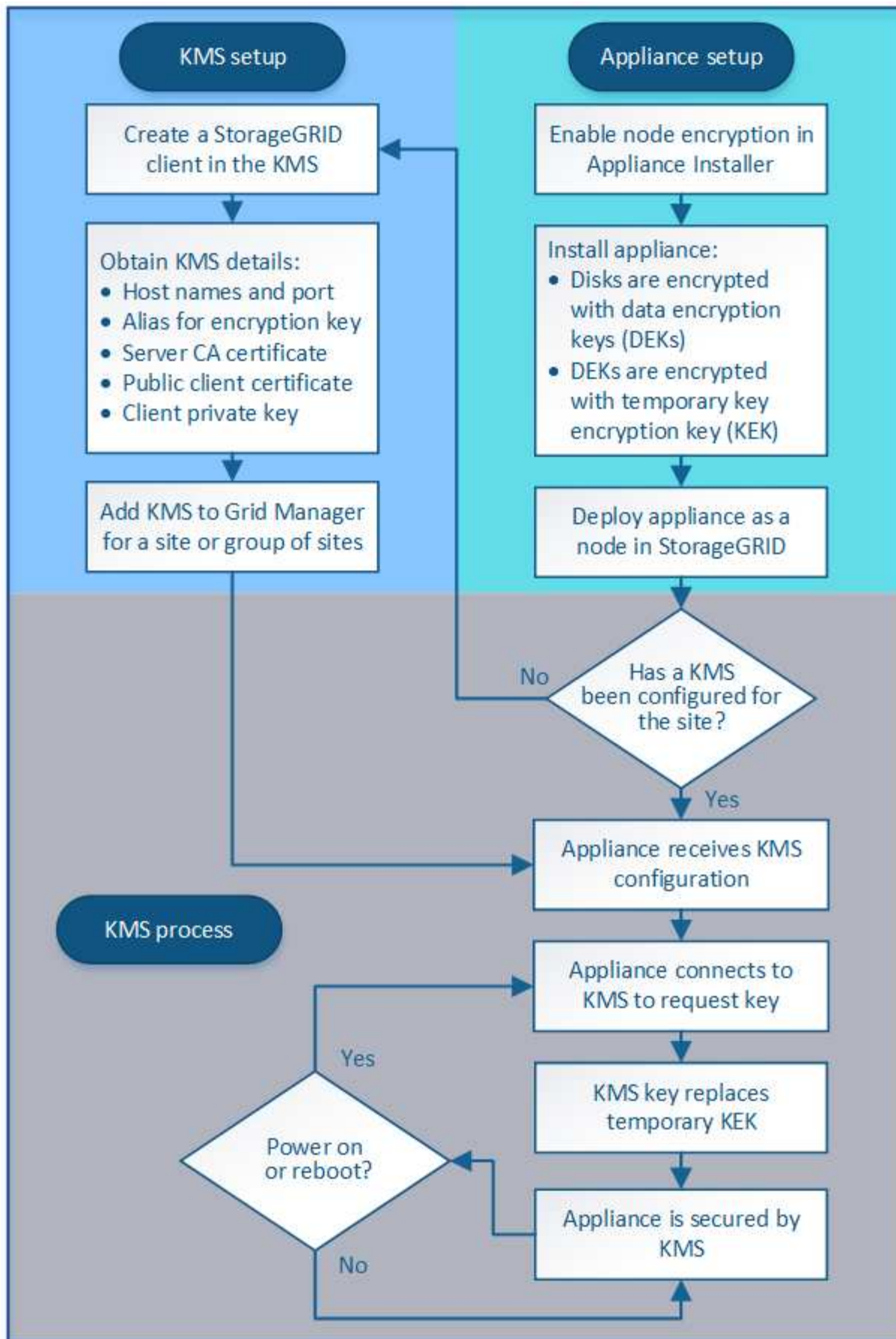
- Vous pouvez utiliser un KMS pour protéger les nœuds d'appliance et utiliser également la fonctionnalité de sécurité des disques de SANtricity System Manager pour « déchiffrer » les données présentes sur les disques à autocryptage des mêmes dispositifs.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds d'appliance et utiliser l'option GRID de chiffrement d'objet stocké pour chiffrer tous les objets à l'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.

Présentation de la configuration des appliances et KMS

Avant d'utiliser un serveur de gestion des clés (KMS) afin de sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds pour les nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés est automatique.

L'organigramme présente les étapes générales permettant d'utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.



L'organigramme présente la configuration du KMS et l'appliance en parallèle. Toutefois, vous pouvez

configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	Configurer StorageGRID en tant que client dans le KMS
Obtenir les informations requises pour le client StorageGRID sur le KMS.	Configurer StorageGRID en tant que client dans le KMS
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	Ajout d'un serveur de gestion des clés (KMS)

Configurez l'appareil

La configuration d'un nœud d'appliance pour l'utilisation de KMS comprend les étapes générales suivantes.

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.



Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille et vous ne pouvez pas utiliser la gestion externe des clés pour les appliances dont le cryptage 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 Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
 - Chaque DEK individuel est chiffré par une clé de 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.

Pour plus de détails, reportez-vous aux sections suivantes :

- [Appareils de services SG100 et SG1000](#)
- [Dispositifs de stockage SG6000](#)
- [Appliances de stockage SG5700](#)
- [Appliances de stockage SG5600](#)

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, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés

Avant de configurer un serveur de gestion des clés externe (KMS), vous devez connaître les considérations et les exigences requises.

Quelles sont les exigences du protocole KMIP ?

StorageGRID prend en charge KMIP version 1.4.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Les communications entre les nœuds d'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID prend en charge le chiffrement TLS v1.2 suivant pour KMIP :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au cluster KMS ou KMS que vous avez configuré pour le site.

Les paramètres de pare-feu réseau doivent permettre à chaque nœud de l'appliance de communiquer via le port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Quels dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être

activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.



Vous ne pouvez pas activer le chiffrement de nœud après l'ajout d'une appliance à la grille et ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement de nœud n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les nœuds d'appliance et les appliances StorageGRID suivants :

Appliance	Type de nœud
Appareil de services SG1000	Nœud d'administration ou nœud de passerelle
Appareil de services SG100	Nœud d'administration ou nœud de passerelle
Dispositif de stockage SG6000	Nœud de stockage
Appliance de stockage SG5700	Nœud de stockage
Appliance de stockage SG5600	Nœud de stockage

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds Software-based (non appliance), notamment :

- 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 ?

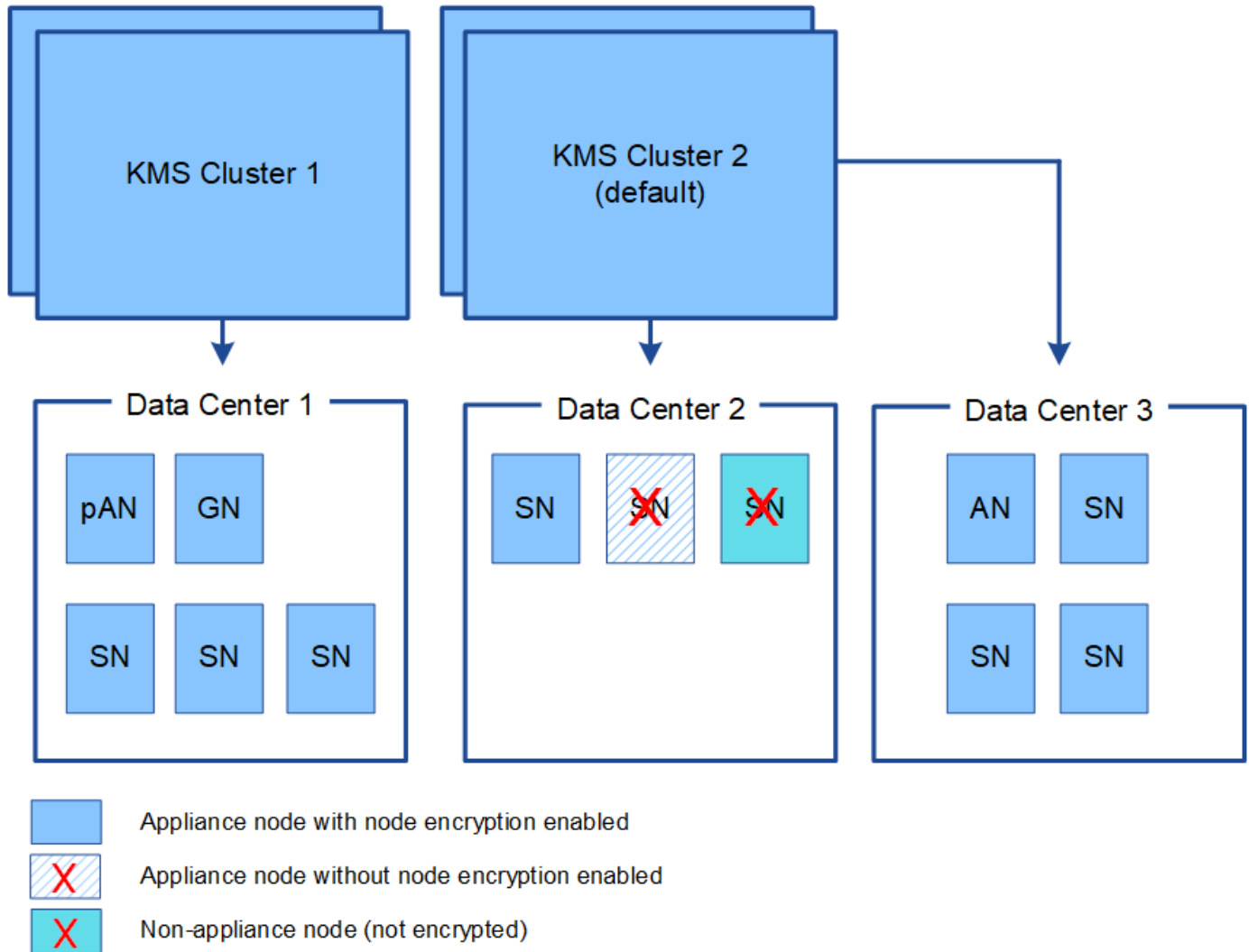
Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés de chiffrement pour les nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une clé de chiffrement unique aux nœuds d'appliance StorageGRID sur un seul site ou dans un groupe de sites.

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-appliance ou pour les nœuds d'appliance dont le paramètre **Node Encryption** n'est pas activé au cours de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

Dans le cadre de nos meilleures pratiques en matière de sécurité, vous devez régulièrement faire tourner la clé de chiffrement utilisée par chaque KMS configuré.

Lors de la rotation de la clé de chiffrement, utilisez le logiciel KMS pour faire pivoter la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne pas tourner sur une clé totalement différente.



Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS dans Grid Manager. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. Utilisez le même alias de clé pour les nouvelles clés que celles utilisées pour les touches précédentes. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour crypter les volumes de l'appliance, l'alerte **KMS échec de rotation de la clé de chiffrement** 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. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour effacer 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.

Informations associées

- [Appareils de services SG100 et SG1000](#)
- [Dispositifs de stockage SG6000](#)
- [Appliances de stockage SG5700](#)
- [Appliances de stockage SG5600](#)

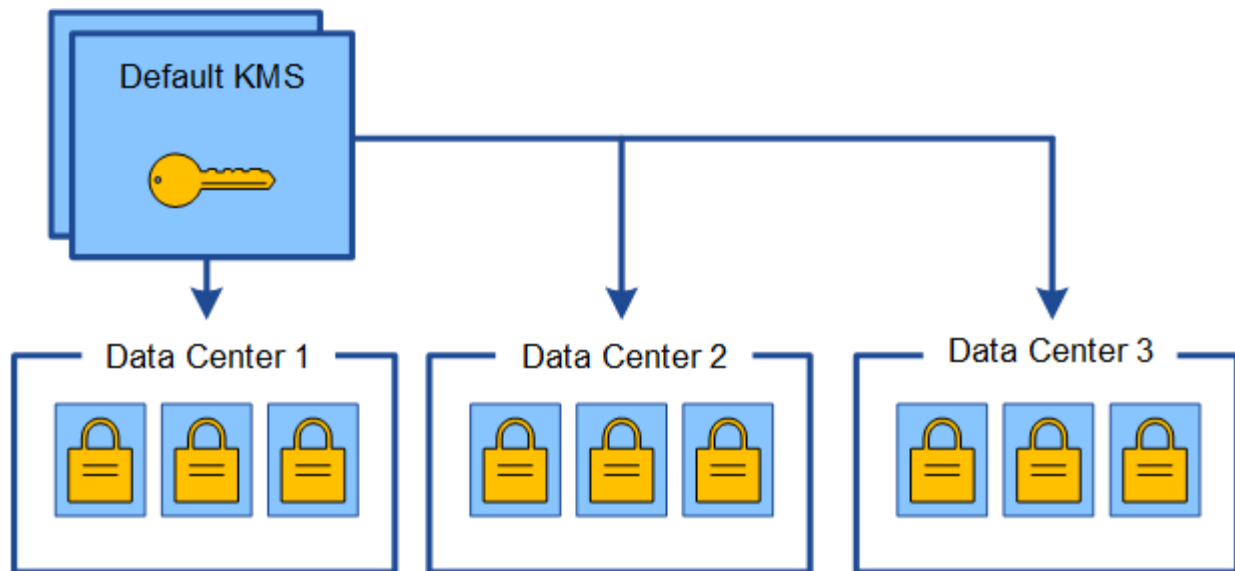
Considérations relatives à la modification du KMS pour un site

Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS vers un autre.

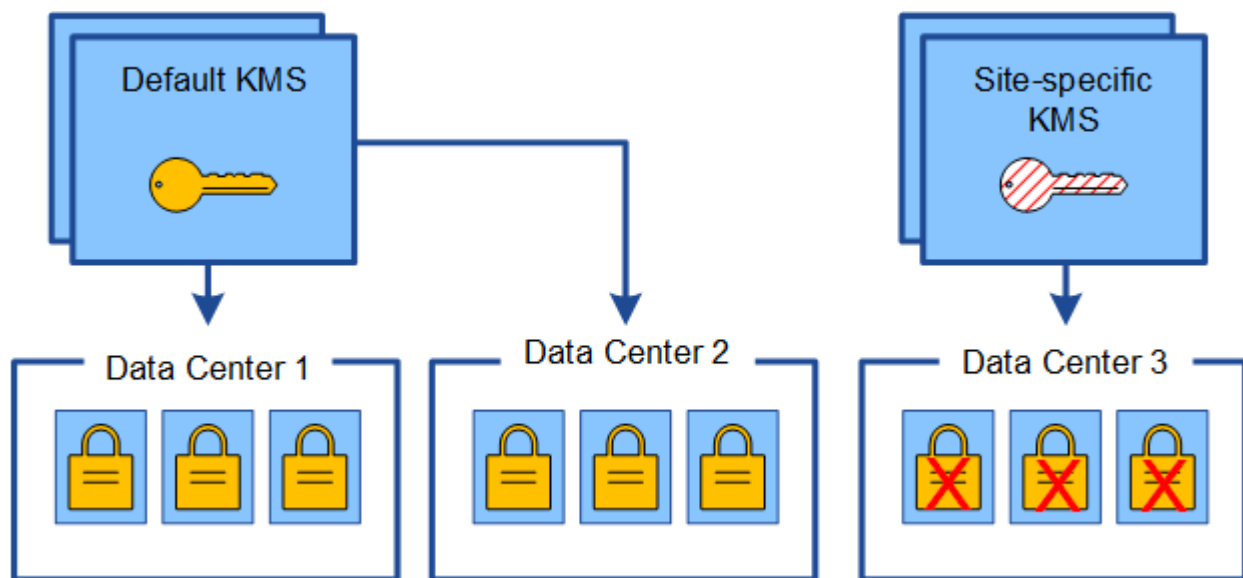
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour décrypter les nœuds de l'appliance chiffrée sur le site.

Par exemple :

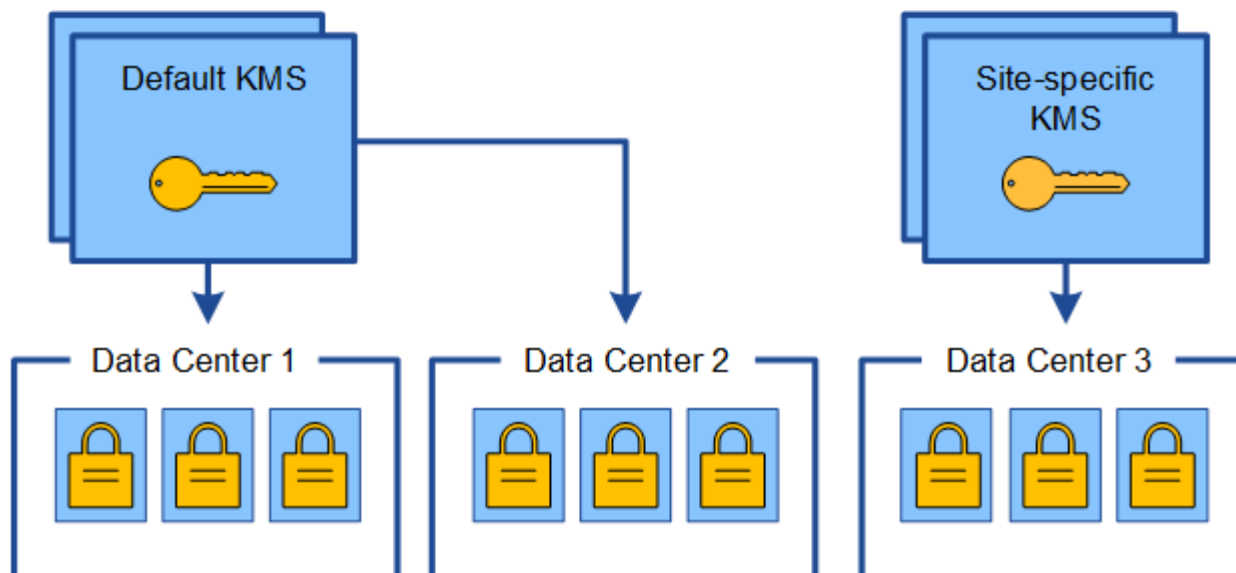
1. Vous configurez au départ un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'appliance sont déjà chiffrés. Une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour décrypter les nœuds d'appliance sur Data Center 3, afin qu'ils puissent être sauvegardés sur StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS pour un site.

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ gère clés pour, sélectionnez sites non gérés par un autre KMS (KMS par défaut). Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. Modification d'un serveur de gestion des clés (KMS)
Vous avez un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds d'appliance du nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. Ajout d'un serveur de gestion des clés (KMS)

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. Ajout d'un serveur de gestion des clés (KMS)

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion externe des clés ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

Description de la tâche

Ces instructions s'appliquent à Thales CipherTrust Manager k170v, versions 2.0, 2.1 et 2.2. Pour toute question concernant l'utilisation d'un autre serveur de gestion des clés avec StorageGRID, contactez le support technique.

"Thales CipherTrust Manager"

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque cluster KMS ou KMS que vous souhaitez utiliser.

Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID dans un seul site ou dans un groupe de sites.

2. Depuis le logiciel KMS, créez une clé de chiffrement AES pour chaque cluster KMS ou KMS.

La clé de cryptage doit être exportable.

3. Notez les informations suivantes pour chaque cluster KMS ou KMS.

Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID.

- Nom d'hôte ou adresse IP pour chaque serveur.
- Port KMIP utilisé par le KMS.
- Alias de clé pour la clé de cryptage dans le KMS.



La clé de chiffrement doit déjà exister dans le KMS. StorageGRID ne crée ni ne gère pas de clés KMS.

4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

- Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.
- Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.



Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer les mêmes FQDN ou adresses IP dans le champ **Hostname**.

- Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.

5. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajout d'un serveur de gestion des clés (KMS)

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque cluster KMS ou KMS.

Ce dont vous avez besoin

- Vous avez passé en revue le [considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés](#).
- Vous avez [Configuration de StorageGRID en tant que client dans le KMS](#), Et vous disposez des informations requises pour chaque cluster KMS ou KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, toutes les appliances chiffrées par nœud dans le grid seront chiffrées par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. Voir [Considérations relatives à la modification du KMS pour un site](#) pour plus d'informations.

Étape 1 : saisissez les détails du KMS

À l'étape 1 (entrer les détails KMS) de l'assistant Ajout d'un serveur de gestion des clés, vous fournissez des détails sur le cluster KMS ou KMS.

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

La page Key Management Server s'affiche avec l'onglet Configuration Details (Détails de la configuration) sélectionné.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?

Key Name ?

Manages keys for ?

Hostname ?

Certificate Status ?

No key management servers have been configured. Select **Create**.

2. Sélectionnez **Créer**.

L'étape 1 (entrer les détails KMS) de l'assistant Ajout d'un serveur de gestion de clés s'affiche.

Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name ?	
Key Name ?	
Manages keys for ?	-- Choose One -- ▾
Port ?	5696
Hostname ?	

+

Cancel

Next

3. Entrez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom d'affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.

Champ	Description
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.
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 ne disposent pas d'un KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. Remarque : Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. Remarque : le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous utilisez un cluster KMS, sélectionnez le signe plus  pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Suivant**.

Étape 2 : télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat de serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au

KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. À partir de **Étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat du serveur enregistré ou du groupe de certificats.

Add a Key Management Server

1

2

3

Enter KMS
Details

Upload
Server
Certificate

Upload Client
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ

Cancel

Back

Next

2. Téléchargez le fichier de certificat.

Les métadonnées du certificat de serveur s'affichent.

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate

k170vCA.pem

Server Certificate Metadata

```
Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79
```



Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat s'affichent sur son propre onglet.

3. Sélectionnez **Suivant**.

Étape 3 : télécharger des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajout d'un serveur de gestion des clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

1. À partir de **Étape 3 (Téléchargement de certificats client)**, accédez à l'emplacement du certificat client.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

Client Certificate Private Key ?

Browse

Cancel

Back

Save

2. Téléchargez le fichier de certificat client.

Les métadonnées du certificat client s'affichent.

3. Accédez à l'emplacement de la clé privée pour le certificat client.

4. Téléchargez le fichier de clé privée.

Les métadonnées du certificat client et de la clé privée du certificat client s'affichent.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Cancel

Back

Save

5. Sélectionnez **Enregistrer**.

Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.



Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur apparaît lorsque vous sélectionnez **Enregistrer**, 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**.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers 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.

- Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Afficher les détails du KMS

Vous pouvez afficher des informations sur chaque serveur de gestion des clés (KMS) de votre système StorageGRID, notamment l'état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés configurés.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Examinez les informations du tableau pour chaque KMS.

Champ	Description
Nom d'affichage DES KMS	Nom descriptif du KMS.

Champ	Description
Nom de clé	Alias de clé pour le client StorageGRID dans le KMS.
Gère les clés pour	Site StorageGRID associé au KMS Ce champ affiche le nom d'un site StorageGRID spécifique ou sites non gérés par un autre KMS (KMS par défaut) .
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion des clés supplémentaires dans le cluster. Par exemple : 10.10.10.10 and 10.10.10.11 ou 10.10.10.10 and 2 others. Pour afficher tous les noms d'hôte d'un cluster, sélectionnez un KMS, puis sélectionnez Modifier .
État du certificat	État actuel du certificat de serveur, du certificat d'autorité de certification facultatif et du certificat client : valide, expiré, proche de l'expiration ou inconnu. Remarque : StorageGRID peut prendre 30 minutes pour obtenir des mises à jour de l'état du certificat. Vous devez actualiser votre navigateur Web pour voir les valeurs actuelles.

3. Si l'état du certificat est inconnu, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.



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 réel.

4. Si la colonne État du certificat indique qu'un certificat a expiré ou qu'il arrive à expiration, traitez le problème dès que possible.

Consultez les actions recommandées pour les alertes d'expiration du certificat CA **KMS**, **expiration du certificat client KMS** et **expiration du certificat serveur KMS** dans les instructions pour [Contrôle et dépannage de StorageGRID](#).



Vous devez corriger tout problème de certificat dès que possible pour maintenir l'accès aux données.

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.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create	Edit	Remove			
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?	
☒ Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid	

2. En haut de la page, sélectionnez l'onglet **Nodes cryptés**.

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

L'onglet nœuds cryptés répertorie les nœuds d'appliance de votre système StorageGRID dont le paramètre **Node Encryption** est activé.

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67 	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

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 d'affichage DES 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 l'intégralité d'un UID de clé, placez le curseur sur la cellule. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de connexion peut prendre plusieurs minutes après la modification de la configuration KMS. Remarque : vous devez actualiser votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

- Echec du chargement de la configuration DES KMS
- Erreur de connectivité KMS

- Nom de la clé de cryptage KMS introuvable
- Echec de la rotation de la clé de chiffrement KMS
- La clé KMS n'a pas réussi à décrypter un volume d'appliance
- LES KMS ne sont pas configurés

Reportez-vous aux actions recommandées pour ces alertes dans les instructions pour [Contrôle et dépannage de StorageGRID](#).



Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Modification d'un serveur de gestion des clés (KMS)

Vous devrez peut-être modifier la configuration d'un serveur de gestion des clés, par exemple si un certificat est sur le point d'expirer.

Ce dont vous avez besoin

- Vous avez passé en revue le [considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés](#).
- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le [Considérations relatives à la modification du KMS pour un site](#).
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

La page Key Management Server s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

[Encrypted Nodes](#)

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Sélectionnez le KMS à modifier et sélectionnez **Modifier**.
3. Vous pouvez également mettre à jour les détails dans **étape 1 (entrer les détails KMS)** de l'assistant

Modifier un serveur de gestion de clés.

Champ	Description
Nom d’affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l’alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l’historique des versions du nouvel alias.  Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l’alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données. Considérations et conditions requises pour l’utilisation d’un serveur de gestion des clés
Gère les clés pour	Si vous modifiez un KMS spécifique au site et que vous n’avez pas déjà un KMS par défaut, vous pouvez sélectionner sites non gérés par un autre KMS (par défaut KMS). 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 au 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 SAN du certificat de serveur doit inclure le FQDN ou l’adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d’un cluster KMS.

- Si vous configurez un cluster KMS, sélectionnez le signe plus  pour ajouter un nom d’hôte pour chaque serveur du cluster.
- Sélectionnez **Suivant**.

L'étape 2 (Télécharger un certificat de serveur) de l'assistant Modifier un serveur de gestion de clés s'affiche.

6. Si vous devez remplacer le certificat de serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Suivant**.

L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion de clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.
9. Sélectionnez **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**.



Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers 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.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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.

Ce dont vous avez besoin

- Vous avez passé en revue le [considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés](#).
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d'appliance lorsque le chiffrement de nœud est activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d'appliance sont activés pour que le chiffrement des nœuds soit activé.

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

La page Key Management Server s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
☒ Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Sélectionnez le bouton radio du KMS que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
3. Passez en revue les éléments à prendre en compte dans la boîte de dialogue d'avertissement.

⚠ Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. Sélectionnez **OK**.

La configuration KMS est supprimée.

Gérer les paramètres proxy

Configurez les paramètres du proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des nœuds finaux externes, tels qu'un nœud final sur Internet.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

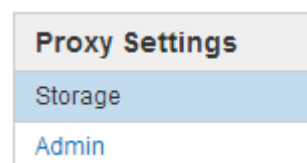
Description de la tâche

Vous pouvez configurer les paramètres d'un proxy de stockage unique.

Étapes

1. Sélectionnez **CONFIGURATION sécurité Paramètres proxy**.

La page Paramètres du proxy de stockage s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.



2. Cochez la case **Activer le proxy de stockage**.

Les champs de configuration d'un proxy de stockage s'affichent.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☒ HTTP ☐ SOCKS5

Hostname

Port (optional)

3. Sélectionnez le protocole du proxy de stockage non transparent.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

Vous pouvez laisser ce champ vide si vous utilisez le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

Une fois le proxy de stockage enregistré, de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud peuvent être configurés et testés.



Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.

Une fois que vous avez terminé

Si vous devez désactiver un proxy de stockage, décochez la case **Activer le proxy de stockage** et sélectionnez **Enregistrer**.

Informations associées

- [Réseau et ports pour les services de plate-forme](#)
- [Gestion des objets avec ILM](#)

Configurez les paramètres du proxy d'administration

Si vous envoyez des messages AutoSupport via HTTP ou HTTPS (reportez-vous à la section [Configurez AutoSupport](#)), vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

Description de la tâche

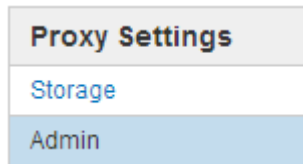
Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

1. Sélectionnez **CONFIGURATION sécurité Paramètres proxy**.

La page Paramètres du proxy administrateur s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Dans le menu barre latérale, sélectionnez **Admin**.



3. Cochez la case **Activer le proxy d'administration**.

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy ☒

Hostname

Port

Username (optional)

Password (optional)

4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir le nom d'utilisateur du proxy.

Laissez ce champ vide si votre serveur proxy ne nécessite pas de nom d'utilisateur.

7. Vous pouvez également saisir le mot de passe du proxy.

Laissez ce champ vide si votre serveur proxy ne nécessite pas de mot de passe.

8. Sélectionnez **Enregistrer**.

Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.



Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

9. Si vous devez désactiver le proxy, décochez la case **Activer le proxy d'administration** et sélectionnez **Enregistrer**.

Gérer les réseaux clients non fiables

Gérer les réseaux clients non approuvés : présentation

Si vous utilisez un réseau client, vous pouvez protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les noeuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. Par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de la grille sur tous les ports externes disponibles (voir les informations sur les communications externes dans le [Instructions de mise en réseau](#)).

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](#).

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 page des noeuds finaux Load Balancer, configurez un noeud final Load Balancer pour S3 sur HTTPS sur le port 443.
2. Dans la page réseaux clients non approuvés, spécifiez que le réseau client sur le nœud de 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 de service de la plateforme S3 sortant à partir d'un nœud de stockage, mais que vous voulez empêcher toute connexion entrante à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans la page réseaux clients non approuvés, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Après avoir enregistré votre configuration, le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais continue d'autoriser les requêtes sortantes vers Amazon Web Services.

Le réseau client du nœud spécifié n'est pas fiable

Si vous utilisez un réseau client, vous pouvez spécifier si le réseau client de chaque nœud est fiable ou non fiable. Vous pouvez également spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

- Vous disposez de l'autorisation d'accès racine.
- Si vous 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.



Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Étapes

1. Sélectionnez **CONFIGURATION sécurité réseaux client non fiables**.

La page réseaux clients non fiables répertorie tous les nœuds de votre système StorageGRID. La colonne motif indisponible comprend une entrée si le réseau client du nœud doit être approuvé.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network
Default ☒ Trusted ☐ Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

☐	Node Name	Unavailable Reason
☐	DC1-ADM1	
☐	DC1-G1	
☐	DC1-S1	
☐	DC1-S2	
☐	DC1-S3	
☐	DC1-S4	
Client Network untrusted on 0 nodes.		

Save

2. Dans la section **Set New Node Default** (définir nouveau nœud par défaut*), indiquez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.
 - **Trusted**: Lorsqu'un nœud est ajouté dans une extension, son réseau client est fiable.
 - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable. Si nécessaire, vous pouvez revenir à cette page pour modifier le paramètre d'un nouveau nœud spécifique.



Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.

3. Dans la section **Sélectionner des nœuds réseau client non approuvés**, sélectionnez les nœuds qui doivent autoriser les connexions client uniquement sur les nœuds finaux de l'équilibreur de charge configurés explicitement.

Vous pouvez sélectionner ou désélectionner la case à cocher du titre pour sélectionner ou désélectionner tous les nœuds.

4. Sélectionnez **Enregistrer**.

Les nouvelles règles de pare-feu sont immédiatement ajoutées et appliquées. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

Gérer les locataires

En tant qu'administrateur du grid, vous créez et gérez les comptes de locataire utilisés par les clients S3 et Swift pour stocker et récupérer des objets, surveiller l'utilisation du stockage et gérer les actions que les clients peuvent exécuter à l'aide de votre système StorageGRID.

Qu'est-ce qu'un compte de locataire ?

Les comptes de locataires permettent aux applications client qui utilisent l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans StorageGRID.

Chaque compte de locataire prend en charge l'utilisation d'un protocole unique, que vous spécifiez lors de la création du compte. Pour stocker et récupérer des objets dans un système StorageGRID avec les deux protocoles, vous devez créer deux comptes de locataire : un pour les compartiments et objets S3, et un pour les conteneurs et objets Swift. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs autorisés, compartiments ou conteneurs, et objets.

Vous pouvez également créer des comptes de tenant supplémentaires si vous souhaitez isoler les objets stockés sur votre système par des entités différentes. Par exemple, vous pouvez définir plusieurs comptes locataires dans l'un de ces cas d'utilisation :

- **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, il vous suffit d'utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Vous n'avez pas besoin d'utiliser de comptes de tenant. Pour plus d'informations, consultez les instructions d'implémentation des applications client S3.

- **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.

Créez et configurez les comptes de locataire

Lorsque vous créez un compte de locataire, vous spécifiez les informations suivantes :

- Afficher le nom du compte locataire.
- Quel protocole client sera utilisé par le compte de locataire (S3 ou Swift).
- Pour les comptes de locataire S3 : si le compte du locataire est autorisé à utiliser des services de plateforme avec des compartiments S3. Si vous autorisez les comptes locataires à utiliser des services de plateforme, vous devez vous assurer que la grille est configurée pour prendre en charge leur utilisation. Voir "Manage des services de plate-forme".
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Si le quota est dépassé, le locataire ne peut pas créer de nouveaux objets.



Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).

- Si la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.

Une fois le compte de locataire créé, vous pouvez effectuer les tâches suivantes :

- **Gérer les services de plate-forme pour le grid** : si vous activez les services de plate-forme pour les comptes de tenant, assurez-vous de comprendre comment les messages de services de plate-forme sont fournis et les exigences de mise en réseau que l'utilisation des services de plate-forme place dans votre déploiement StorageGRID.
- **Surveiller l'utilisation du stockage d'un compte locataire** : lorsque les locataires commencent à utiliser leurs comptes, vous pouvez utiliser Grid Manager pour surveiller la quantité de stockage consommée par chaque locataire.



Les valeurs d'utilisation du stockage d'un locataire peuvent devenir obsolètes si les nœuds sont isolés des autres nœuds de la grille. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

Si vous avez défini des quotas pour les locataires, vous pouvez activer l'alerte **usage du quota de locataires élevé** pour déterminer si les locataires consomment leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour plus d'informations, consultez la référence des alertes dans les instructions de surveillance et de dépannage de StorageGRID.

- **Configurer les opérations client** : vous pouvez configurer si certains types d'opérations client sont interdits.

Configurez les locataires S3

Une fois le compte de locataire S3 créé, les utilisateurs peuvent accéder au Gestionnaire des locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux

- Gestion des clés d'accès S3
- Création et gestion des compartiments S3
- Contrôle de l'utilisation du stockage
- Utilisation des services de plate-forme (si activé)



Les locataires S3 peuvent créer et gérer des compartiments et des clés d'accès S3 avec le gestionnaire des locataires. Cependant, ils doivent utiliser une application client S3 pour récupérer et gérer les objets.

Configurez les locataires Swift

Une fois le compte de locataire Swift créé, l'utilisateur root du locataire peut accéder au Gestionnaire de locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux
- Contrôle de l'utilisation du stockage



Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au Gestionnaire de locataires. Toutefois, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Informations associées

[Utilisez un compte de locataire](#)

Créer un compte de locataire

Vous devez créer au moins un compte de locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Lorsque vous créez un compte de locataire, vous spécifiez un nom, un protocole client et, éventuellement, un quota de stockage. Si l'authentification unique (SSO) est activée pour StorageGRID, vous spécifiez également le groupe fédéré disposant d'une autorisation d'accès racine pour configurer le compte du locataire. Si StorageGRID n'utilise pas la connexion unique, vous devez également indiquer si le compte de tenant utilisera son propre référentiel d'identité et configurer le mot de passe initial de l'utilisateur racine local du locataire.

Grid Manager fournit un assistant qui vous guide dans les étapes de création d'un compte de tenant. Les étapes varient en fonction du cas ou non [fédération des identités](#) et [authentification unique](#). Sont configurés et si le compte Grid Manager que vous utilisez pour créer le compte de tenant appartient à un groupe d'administration disposant de l'autorisation d'accès racine.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- 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'attribuer des autorisations Grid Manager à ce groupe d'administration. Voir la [instructions de gestion des groupes d'administration](#).

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer** et entrez les informations suivantes pour le locataire :
 - a. **Nom** : saisissez un nom pour le compte du locataire. Les noms de locataires ne doivent pas être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.
 - b. **Description** (facultatif) : saisissez une description qui vous aide à identifier le locataire.
 - c. **Type de client** : sélectionnez le type de client **S3** ou **Swift**.
 - d. **Quota de stockage** (facultatif) : si vous souhaitez que ce locataire dispose d'un quota de stockage, entrez une valeur numérique pour le quota et sélectionnez les unités correctes (Go, To ou PB).

Create a tenant

1 Enter details — 2 Select permissions — 3 Define root access

Enter tenant details

Name ?

Description (optional) ?

Client type ?

☒ S3 ☐ Swift

Storage quota (optional) ?

GB ▼

Cancel Continue

3. Sélectionnez **Continuer** et configurez le locataire S3 ou Swift.

Locataire S3

Sélectionnez les autorisations appropriées pour le locataire. Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, consultez l'aide en ligne de chaque autorisation.

- Autoriser les services de plate-forme
- Utiliser son propre référentiel d'identité (sélectionnable uniquement si SSO n'est pas utilisé)
- Autoriser la sélection S3 (voir [Gérez S3 Select pour les comptes de locataires](#))

Locataire Swift

Si le locataire utilise son propre référentiel d'identité, sélectionnez **utiliser son propre référentiel d'identité** (sélectionnable uniquement si SSO n'est pas utilisé).

1. Sélectionnez **Continuer** et définissez l'accès racine pour le compte de tenant.

fédération des identités non configurée

1. Entrez un mot de passe pour l'utilisateur racine local.
2. Sélectionnez **Créer locataire**.

SSO activé

Lorsque SSO est activé pour StorageGRID, le locataire doit utiliser le référentiel d'identité qui a été configuré pour le Gestionnaire de grille. Aucun utilisateur local ne peut se connecter. Vous spécifiez le groupe fédéré disposant d'une autorisation d'accès racine pour configurer le compte locataire.

1. Sélectionnez un groupe fédéré existant dans Grid Manager pour obtenir l'autorisation d'accès racine initiale du locataire.



Si vous disposez des autorisations adéquates, les groupes fédérés existants dans Grid Manager sont répertoriés lorsque vous sélectionnez le champ. Sinon, entrez le nom unique du groupe.

2. Sélectionnez **Créer locataire**.

SSO non activé

1. Suivez les étapes décrites dans le tableau selon que le locataire gère ses propres groupes et utilisateurs ou utilise le référentiel d'identité qui a été configuré pour Grid Manager.

Si le locataire va...	Procédez comme ça...
Gérez ses propres groupes et utilisateurs	a. Sélectionnez utiliser son propre référentiel d'identité. Remarque : si cette case est cochée et que vous souhaitez utiliser la fédération des identités pour les groupes de locataires et les utilisateurs, le locataire doit configurer son propre référentiel d'identité. Voir la instructions d'utilisation des comptes de tenant. b. Spécifiez un mot de passe pour l'utilisateur racine local du locataire, puis sélectionnez Créer locataire. c. Sélectionnez se connecter en tant que root pour configurer le locataire, ou sélectionnez Terminer pour le configurer ultérieurement.
Utilisez les groupes et utilisateurs configurés pour le Grid Manager	a. Effectuez l'une des opérations suivantes ou les deux : ◦ Sélectionnez un groupe fédéré existant dans le Grid Manager qui doit avoir l'autorisation d'accès racine initiale pour le locataire. Remarque : si vous disposez d'autorisations adéquates, les groupes fédérés existants du Gestionnaire de grille sont répertoriés lorsque vous sélectionnez le champ. Sinon, entrez le nom unique du groupe. ◦ Spécifiez un mot de passe pour l'utilisateur racine local du locataire. b. Sélectionnez Créer locataire.

1. Pour vous connecter au locataire maintenant :

- Si vous accédez à Grid Manager sur un port restreint, sélectionnez **restreint** dans le tableau locataire pour en savoir plus sur l'accès à ce compte de tenant.

L'URL du Gestionnaire de locataires a le format suivant :

`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`

- *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration
 - *port* est le port locataire uniquement
 - *20-digit-account-id* Est l'ID de compte unique du locataire
- Si vous accédez au Gestionnaire de grille sur le port 443 mais que vous n'avez pas défini de mot de passe pour l'utilisateur racine local, dans la table des locataires du Gestionnaire de grille, sélectionnez **se connecter** et entrez les informations d'identification pour un utilisateur dans le groupe fédéré d'accès racine.
 - Si vous accédez à Grid Manager sur le port 443 et que vous définissez un mot de passe pour l'utilisateur racine local :
 - i. Sélectionnez **se connecter en tant que root** pour configurer le tenant maintenant.

Lorsque vous vous connectez, des liens apparaissent pour configurer des compartiments ou des conteneurs, la fédération des identités, les groupes et les utilisateurs.

×

Create a tenant

✓ Enter details

✓ Select permissions

✓ Define root access



The tenant Tenant02 was created.

If you're ready to configure the tenant, select **Sign in as root**.

Sign in as root

✓ Signed in

You can now access the Tenant Manager to configure these settings:

- **Buckets**  : Create and manage buckets.
- **Identity federation**  : Configure an external identity source to use federated groups.
- **Groups**  : Manage groups and assign permissions.
- **Users**  : Manage local users and assign users to groups.

Finish

i. Sélectionnez les liens pour configurer le compte de tenant.

Chaque lien ouvre la page correspondante dans le Gestionnaire de locataires. Pour terminer la page, reportez-vous à la section [instructions d'utilisation des comptes de tenant](#).

ii. Sinon, sélectionnez **Finish** pour accéder au locataire ultérieurement.

2. Pour accéder au locataire ultérieurement :

Si vous utilisez...	Effectuez l'une d'entre elles...
Orifice 443	• Dans Grid Manager, sélectionnez TENANTS, puis connexion à droite du nom du locataire. • Entrez l'URL du locataire dans un navigateur Web : ° <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code> ° <code>FQDN_or_Admin_Node_IP</code> Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ° <code>20-digit-account-id</code> Est l'ID de compte unique du locataire

Si vous utilisez...	Effectuez l'une d'entre elles...
Un port restreint	- Dans le Gestionnaire de grille, sélectionnez TENANTS et sélectionnez restreint. - Entrez l'URL du locataire dans un navigateur Web : <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

Informations associées

- [Contrôle de l'accès par le biais de pare-feu](#)
- [Gestion des services de plateforme pour les comptes de locataires S3](#)

Modifiez le mot de passe de l'utilisateur racine local du locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si celui-ci est verrouillé hors du compte.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte du 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

Search tenants by name or ID

Q

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Sélectionnez le compte de locataire à modifier.

Le bouton actions est activé.

3. Dans la liste déroulante **actions**, sélectionnez **changer mot de passe racine**.

4. Saisissez le nouveau mot de passe du compte de tenant.

5. Sélectionnez **Enregistrer**.

Modifiez le compte de tenant

Vous pouvez modifier un compte de tenant pour modifier le nom d’affichage, modifier le paramètre du référentiel d’identité, autoriser ou interdire les services de plate-forme, ou entrer un quota de stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l’aide d’un [navigateur web pris en charge](#).
- Vous disposez d’autorisations d’accès spécifiques.

Étapes

1. Sélectionnez **LOCATAIRES**.

Tenants

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

Create

Export to CSV

Actions

Search tenants by name or ID

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Sélectionnez le compte de locataire à modifier.

Utilisez la zone de recherche pour rechercher un compte de locataire par nom ou ID de locataire.

3. Dans la liste déroulante actions, sélectionnez **Modifier**.

Cet exemple concerne une grille qui n'utilise pas SSO (Single Sign-on). Ce compte de tenant n'a pas configuré son propre référentiel d'identité.

×

Edit the tenant

1 Enter details

✓ Select permissions

Enter tenant details

Name ?

Tenant 01

Description (optional) ?

Description

Client type ?

☒ S3
☐ Swift

Storage quota (optional) ?

GB ▼

Cancel

Continue

4. Modifiez les valeurs de ces champs comme requis :

- **Nom**
- **Description**
- **Type de client**
- **Quota de stockage**

5. Sélectionnez **Continuer**.

6. Sélectionner ou désélectionner 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.
- Modifiez le paramètre de la case à cocher **utilise son propre référentiel d'identité** pour déterminer si le compte de tenant utilisera son propre référentiel d'identité ou le référentiel d'identité qui a été configuré pour le gestionnaire de grille.

Si la case à cocher **utilise son propre référentiel d'identité** est :

- Désactivé et coché, 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 décoché, la fonctionnalité SSO est activée pour le système StorageGRID. Le locataire doit utiliser le référentiel d'identité qui a été configuré pour Grid Manager.
- Activez ou désactivez **S3 Select** selon les besoins. Voir [Gérez S3 Select pour les comptes de locataires](#).

7. Sélectionnez **Enregistrer**.

Informations associées

- [Gestion des services de plateforme pour les comptes de locataires S3](#)
- [Utilisez un compte de locataire](#)

Supprimer le compte de locataire

Vous pouvez supprimer un compte de tenant si vous souhaitez supprimer définitivement l'accès du tenant au système.

Ce dont vous avez besoin

- Vous devez être connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir supprimé tous les compartiments (S3), les conteneurs (Swift) et les objets associés au compte du locataire.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez le compte de tenant que vous souhaitez supprimer.

Utilisez la zone de recherche pour rechercher un compte de locataire par nom ou ID de locataire.

3. Dans la liste déroulante **actions**, sélectionnez **Supprimer**.
4. Sélectionnez **OK**.

Gestion des services de plateforme

Gestion des services de plateforme pour les comptes de locataires S3

Si vous activez des services de plateforme pour les comptes de locataires S3, vous devez configurer votre grid de manière à ce que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Qu'est-ce que les services de plateforme ?

Les services de plateforme incluent la réplication CloudMirror, les notifications d'événement et le service d'intégration de la recherche.

Ces services permettent aux locataires d'utiliser les fonctionnalités suivantes avec leurs compartiments S3 :

- **Réplication CloudMirror** : le service de réplication StorageGRID CloudMirror permet la mise en miroir d'objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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



La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.

- **Notifications** : les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un service externe Amazon simple notification Service™ (SNS) spécifié.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.



Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- **Service d'intégration de recherche** : le service d'intégration de recherche est utilisé pour envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.



Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Les services de plateforme permettent aux locataires d'utiliser des ressources de stockage externes, des services de notification et des services de recherche ou d'analyse avec leurs données. Étant donné que l'emplacement cible des services de plateforme ne fait généralement pas partie de votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Dans ce cas, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes de tenant. Vous devez également configurer votre réseau de sorte que les messages de services de plate-forme générés par les locataires puissent atteindre leurs destinations.

Recommandations relatives à l'utilisation des services de plate-forme

Avant d'utiliser les services de plate-forme, tenez compte des recommandations suivantes :

- Si le contrôle de versions et la réplication CloudMirror sont activés pour un compartiment S3 dans le système StorageGRID, vous devez également activer la gestion des versions du compartiment S3 pour le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Les demandes vers un noeud final qui ne peut pas être terminé seront mises en file d'attente jusqu'à un maximum de 500,000 requêtes. Cette limite est également partagée entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500,000 de sorte que les locataires nouvellement créés ne sont pas pénalisés injustement.

Informations associées

- [Utilisez un compte de locataire](#)
- [Configurez les paramètres du proxy de stockage](#)
- [Surveiller et résoudre les problèmes](#)

Réseau et ports pour les services de plate-forme

Si vous autorisez un locataire S3 à utiliser des services de plateforme, vous devez configurer la mise en réseau pour le grid de manière à ce que les messages des services de plateforme puissent être envoyés vers leur destination.

Lorsque vous créez ou mettez à jour le compte de locataire, vous pouvez activer des services de plateforme pour un compte de locataire S3. Si les services de plateforme sont activés, le locataire peut créer des terminaux qui servent de destination à la réplication CloudMirror, à la notification d'événement ou aux messages d'intégration de recherche à partir de ses compartiments S3. Ces messages de services de plateforme sont envoyés depuis les nœuds de stockage qui exécutent le service ADC vers les terminaux de destination.

Par exemple, les locataires peuvent configurer les types de terminaux de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Application locale prenant en charge la réception de messages SNS (simple notification Service)
- Un compartiment S3 hébergé localement sur la même instance d'StorageGRID ou sur une autre instance
- Un terminal externe, tel qu'un terminal sur Amazon Web Services.

Pour vous assurer que les messages des services de plate-forme peuvent être envoyés, vous devez configurer le réseau ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer des messages de services de plate-forme aux nœuds finaux de destination.

Par défaut, les messages des services de plate-forme sont envoyés sur les ports suivants :

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

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un 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.

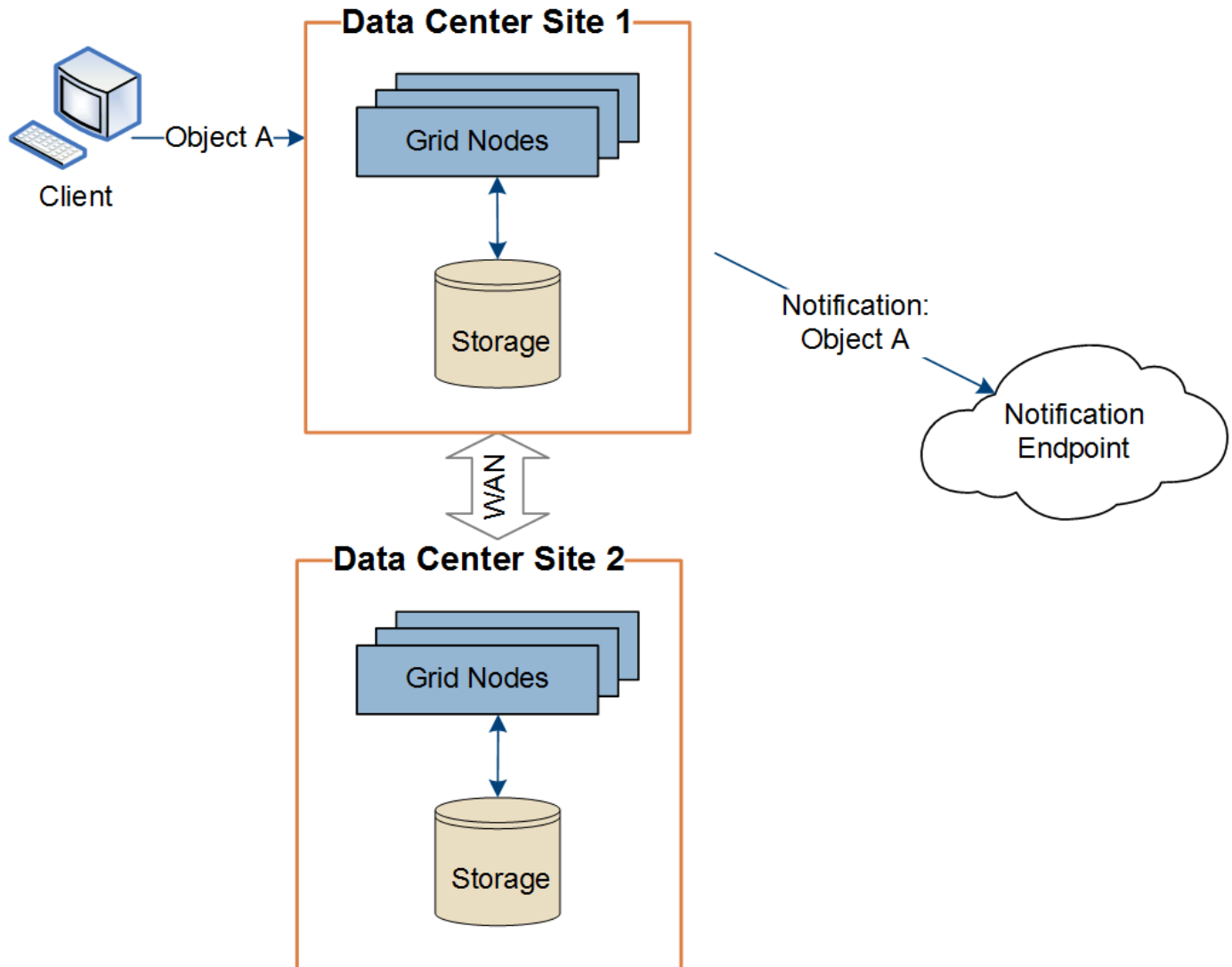
Si vous utilisez un serveur proxy non transparent, vous devez également [Configurer les paramètres du proxy de stockage](#) pour permettre l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur internet.

Informations associées

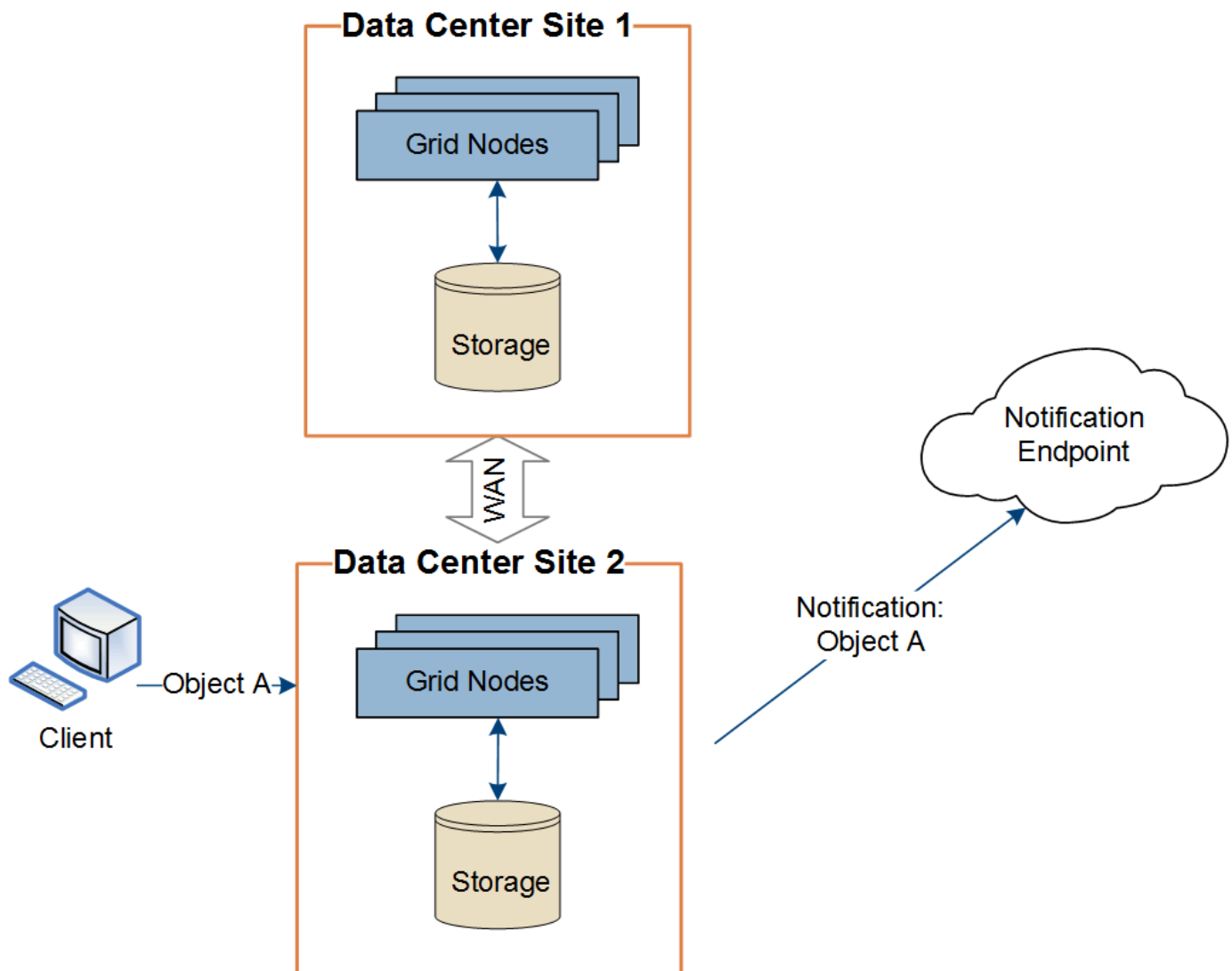
- [Utilisez un compte de locataire](#)

Toutes les opérations de services de plateforme sont réalisées sur une base par site.

C'est-à-dire que si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle sur le site de Data Center 1, la notification concernant cette action est déclenchée et envoyée depuis le site de Data Center 1.



Si le client exécute ensuite une opération de suppression d'API S3 sur ce même objet à partir du site du centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis le site du centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de plate-forme puissent être transmis à leurs destinations.

Résoudre les problèmes liés aux services de plateforme

Les terminaux utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le Gestionnaire de locataires. Toutefois, si un locataire a des problèmes de configuration ou d'utilisation des services de plateforme, vous pouvez utiliser le Gestionnaire de grille pour résoudre le problème.

Problèmes liés aux nouveaux terminaux

Avant qu'un locataire ne puisse utiliser les services de plateforme, il doit créer un ou plusieurs terminaux à l'aide du Gestionnaire des locataires. Chaque terminal représente une destination externe pour un service de plateforme unique, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un thème simple Service de notification ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque noeud final comprend à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un noeud final, le système StorageGRID valide que ce dernier existe et qu'il peut être atteint à l'aide des identifiants spécifiés. La connexion au noeud final est validée à partir d'un nœud sur chaque

site.

Si la validation du noeud final échoue, un message d'erreur explique pourquoi la validation du noeud final a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer de créer à nouveau le noeud final.



La création de point final échoue si les services de plate-forme ne sont pas activés pour le compte de locataire.

Problèmes avec les terminaux existants

En cas d'erreur lorsqu'StorageGRID tente d'atteindre un terminal 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 noeuds finaux pour consulter le message d'erreur le plus récent pour chaque noeud final et déterminer la durée de l'erreur. La colonne **dernière erreur** affiche le message d'erreur le plus récent pour chaque noeud final et indique la durée de l'erreur. Erreurs incluant le  l'icône s'est produite au cours des 7 derniers jours.

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 des nœuds de stockage et des terminaux de service de plateforme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy afin de vous assurer que les messages relatifs au service de la plate-forme ne sont pas bloqués.

Déterminez si une erreur s'est produite

Si des erreurs de point final se sont produites au cours des 7 derniers jours, le tableau de bord du Gestionnaire des locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux pour obtenir plus de détails sur l'erreur.

Échec des opérations client

Certains problèmes de service de plateforme peuvent entraîner l'échec des opérations client dans le compartiment S3. Par exemple, les opérations client S3 échouent si le service RSM (Replicated State machine) interne s'arrête ou s'il y a trop de messages de services de plate-forme en file d'attente pour la livraison.

Pour vérifier l'état des services :

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **site Storage Node SSM Services**.

Erreurs récupérables et récupérables du point final

Une fois les noeuds finaux créés, des erreurs de demande de service de plate-forme peuvent se produire pour diverses raisons. Certaines erreurs peuvent être récupérées avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent se produire pour les raisons suivantes :

- Les informations d'identification de l'utilisateur ont été supprimées ou ont expiré.
- Le compartiment de destination n'existe pas.
- La notification ne peut pas être envoyée.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plate-forme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le noeud final est supprimé.

Si StorageGRID rencontre une erreur de point final irrécupérable, l'alarme d'événements totaux (SMTT) héritée est déclenchée dans le Gestionnaire de grille. Pour afficher l'alarme Total Events hérité :

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **site node SSM Events**.
3. Afficher le dernier événement en haut du tableau.

Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

4. Suivez les instructions fournies dans le contenu de l'alarme SMTT pour corriger le problème.
5. Sélectionnez l'onglet **Configuration** pour réinitialiser le nombre d'événements.

6. Notifier le locataire des objets dont les messages de services de plate-forme n'ont pas été livrés.
7. Demandez au locataire de déclencher à nouveau la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou balises de l'objet.

Le locataire peut soumettre de nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Les messages des services de plate-forme ne peuvent pas être transmis

Si la destination rencontre un problème qui l'empêche d'accepter des messages de services de plate-forme, l'opération client sur le compartiment réussit, mais le message des services de plate-forme n'est pas livré. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination de sorte que StorageGRID ne puisse plus s'authentifier auprès du service de destination.

Si les messages des services de la plate-forme ne peuvent pas être envoyés en raison d'une erreur irrécupérable, l'alarme Total Events (SMTT) TDA/TDE/MMS (Total Events (SMTT) TDA/TDE) se déclenche dans le Grid Manager.

Des performances plus lentes pour les demandes de services de plateforme

Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination.

Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'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 **NOEUDS**.
2. Sélectionnez **site Platform Services**.
3. Afficher le tableau des taux d'erreur de demande.



Alerte de services de plate-forme non disponibles

L'alerte **Platform services unavailable** indique qu'aucune opération de service de plate-forme ne peut être effectuée sur un site car trop de nœuds de stockage avec le service RSM sont en cours d'exécution ou 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 que la plupart de ces nœuds de stockage sont exécutés et disponibles.



Si plusieurs nœuds de stockage contenant le service RSM échouent sur un site, vous perdez toute demande de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les terminaux des services de plateforme

Pour plus d'informations sur le dépannage des terminaux de services de plate-forme, reportez-vous aux instructions de la section [utilisation d'un compte de locataire](#).

Informations associées

- [Surveiller et résoudre les problèmes](#)
- [Configurez les paramètres du proxy de stockage](#)

Gérez S3 Select pour les comptes de locataires

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes SelectObjectContent sur des objets individuels.

S3 Select constitue un moyen efficace d'effectuer des recherches dans de vastes volumes de données sans avoir à déployer une base de données et les ressources associées pour activer les recherches. Il réduit également le coût et la latence liés à la récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser les requêtes SelectObjectContent pour filtrer et récupérer uniquement les données nécessaires à partir d'un objet. L'implémentation d'StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et configuration requise pour l'utilisation de S3 Select

StorageGRID nécessite les éléments suivants pour les requêtes S3 Select :

- L'objet que vous souhaitez interroger est au format CSV ou est un fichier compressé GZIP ou BZIP2 contenant un fichier au format CSV.
- Les locataires doivent obtenir la possibilité S3 Select de l'administrateur du grid. Sélectionnez **Autoriser sélection S3** quand [création d'un locataire](#) ou [modification d'un locataire](#).
- La requête 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 des nœuds d'appliance SG100 ou SG1000 ou des nœuds logiciels VMware.

Notez les limites suivantes :

- Les nœuds d'équilibrage de la charge sans système d'exploitation ne sont pas pris en charge.
- Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.
- Les requêtes envoyées via le service CLB obsolète ne sont pas prises en charge.



SelectObjectContent les demandes peuvent réduire les performances d'équilibrage de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

Voir la [Instructions d'utilisation de S3 Select](#).

Pour afficher [Graphiques Grafana](#) Pour les opérations S3 Select dans le temps, sélectionnez **SUPPORT Outils métriques** dans le gestionnaire de grille.

Configurez les connexions des clients S3 et Swift

À propos des connexions des clients S3 et Swift

En tant qu'administrateur grid, vous gérez les options de configuration qui contrôlent la manière dont les locataires S3 et Swift peuvent connecter les applications client à votre système StorageGRID pour stocker et récupérer les données. Plusieurs options sont possibles pour répondre aux différents besoins des clients et des locataires.

Les applications client peuvent stocker ou récupérer des objets en se connectant à l'un des éléments suivants :

- Le service Load Balancer sur les nœuds d'administration ou de passerelle, ou, le cas échéant, l'adresse IP virtuelle d'un groupe de nœuds d'administration ou de nœuds de passerelle haute disponibilité
- Le service CLB sur les nœuds de passerelle ou, éventuellement, l'adresse IP virtuelle d'un groupe de nœuds de passerelle haute disponibilité



Le service CLB est obsolète. Les clients configurés avant la version de StorageGRID 11.3 peuvent continuer à utiliser le service CLB sur les nœuds de passerelle. Toutes les autres applications client qui dépendent de StorageGRID pour fournir un équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Vous pouvez choisir de configurer les fonctions suivantes sur votre système StorageGRID :

- **Interfaces VLAN** : vous pouvez créer des interfaces VLAN (Virtual LAN) sur les nœuds d'administration et les nœuds de passerelle pour isoler et partitionner le trafic client et locataire afin d'assurer la sécurité, la flexibilité et les performances. Après avoir créé une interface VLAN, vous l'ajoutez à un groupe haute disponibilité (HA).
- **Groupe haute disponibilité** : vous pouvez créer un groupe haute disponibilité des interfaces pour les nœuds de passerelle ou les nœuds d'administration pour créer une configuration de sauvegarde active/active, ou utiliser le DNS Round-Robin ou un équilibreur de charge tiers et plusieurs groupes haute disponibilité pour obtenir une configuration active/active. Les connexions des clients sont établies en utilisant les adresses IP virtuelles des groupes haute disponibilité.
- **Load Balancer service** : vous pouvez permettre aux clients d'utiliser le service Load Balancer en créant des nœuds finaux load Balancer pour les connexions client. Lors de la création d'un nœud final d'équilibrage de charge, vous spécifiez un numéro de port, que le nœud final accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le nœud final et le certificat à utiliser pour les connexions HTTPS (le cas échéant).
- **Réseau client non fiable** : vous pouvez sécuriser le réseau client en le configurant comme non fiable. Lorsque le réseau client n'est pas fiable, les clients peuvent uniquement se connecter à l'aide de points finaux d'équilibreur de charge.

Vous pouvez également activer l'utilisation du protocole HTTP pour les clients qui se connectent à StorageGRID directement aux nœuds de stockage ou à l'aide du service CLB (obsolète) et vous pouvez configurer les noms de domaine de points de terminaison de l'API S3 pour les clients S3.

Résumé : adresses IP et ports pour les connexions client

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Description de la tâche

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. Ces instructions décrivent la recherche de ces informations dans le grid Manager si les terminaux d'équilibrage de la charge et les groupes haute disponibilité sont déjà configurés.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	• Port du terminal de l'équilibreur de charge
Groupe HAUTE DISPONIBILITÉ	CLB Note: le service CLB est obsolète.	Adresse IP virtuelle d'un groupe haute disponibilité	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084 Ports Swift par défaut : • HTTPS:8083 • HTTP : 8085
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	CLB Note: le service CLB est obsolète.	Adresse IP du nœud de passerelle Remarque : par défaut, les ports HTTP pour CLB et LDR ne sont pas activés.	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084 Ports Swift par défaut : • HTTPS:8083 • HTTP : 8085

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP : 18084 Ports Swift par défaut : • HTTPS: 18083 • HTTP : 18085

Exemples

Pour connecter un client S3 au terminal Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme illustré ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.5 et le numéro de port d'un terminal S3 Load Balancer est 10443, un client S3 peut utiliser l'URL suivante pour vous connecter à StorageGRID :

- `https://192.0.2.5:10443`

Pour connecter un client Swift au point de terminaison Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.6 et que le numéro de port d'un nœud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
2. Pour trouver l'adresse IP d'un nœud de grille :
 - a. Sélectionnez **NOEUDS**.
 - b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.
 - c. Sélectionnez l'onglet **Aperçu**.
 - d. Dans la section informations sur le nœud, notez les adresses IP du nœud.
 - e. Sélectionnez **Afficher plus** pour afficher les adresses IPv6 et les mappages d'interface.

Vous pouvez établir des connexions entre les applications client et n'importe quelle adresse IP de la liste :

- **Eth0:** réseau de grille
- **Eth1:** réseau d'administration (facultatif)
- **Eth2:** réseau client (facultatif)



Si vous affichez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe haute disponibilité, l'adresse IP virtuelle du groupe haute disponibilité est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe haute disponibilité :

- Sélectionnez **CONFIGURATION réseau groupes haute disponibilité**.
- 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 :

- Sélectionnez **CONFIGURATION réseau points d'extrémité de l'équilibreur de charge**.

La page Load Balancer Endpoints s'affiche et affiche la liste des nœuds finaux qui ont déjà été configurés.

- Sélectionnez un nœud final et sélectionnez **Modifier le nœud final**.

La fenêtre Modifier le point final s'ouvre et affiche des informations supplémentaires sur le point final.

- Vérifiez que le nœud final que vous avez sélectionné est configuré pour une utilisation avec le protocole correct (S3 ou Swift), puis sélectionnez **Annuler**.
- Notez le numéro de port du nœud final que vous souhaitez utiliser pour une connexion client.



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.

Configurez les interfaces VLAN

Vous pouvez créer des interfaces VLAN sur des nœuds d'administration et de passerelle et les utiliser dans des groupes haute disponibilité et des terminaux d'équilibrage de la charge pour isoler et partitionner le trafic afin d'assurer la sécurité, la flexibilité et les performances.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en entrant un ID VLAN et en choisissant une interface parent sur un ou plusieurs nœuds.
- Une interface parent doit être configurée comme une interface de ligne réseau au niveau du commutateur.
- Une interface parent peut être la Grid Network (eth0), le réseau client (eth2) ou une interface de ligne de jonction supplémentaire pour la VM ou l'hôte bare-Metal (par exemple, en256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parent pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface réseau Grid et l'interface réseau client sur le même nœud passerelle que l'interface parent pour le même VLAN.

- Si l'interface VLAN est destinée au trafic du nœud d'administration, qui inclut le trafic lié au Grid Manager et au Gestionnaire de locataires, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si l'interface VLAN est destinée au trafic client S3 ou Swift, sélectionnez les interfaces dans les nœuds d'administration ou les nœuds de passerelle.
- Si vous avez besoin d'ajouter des interfaces de jonction, consultez les informations suivantes :
 - **VMware (après l'installation du nœud)** : [VMware : ajoutez du jonction ou des interfaces d'accès à un nœud](#)
 - **RHEL ou CentOS (avant d'installer le nœud)** : [Créez des fichiers de configuration de nœud](#)
 - **Ubuntu ou Debian (avant d'installer le nœud)** : [Créez des fichiers de configuration de nœud](#)
 - **RHEL, CentOS, Ubuntu ou Debian (après l'installation du nœud)** : [Linux : ajoutez une jonction ou des interfaces d'accès à un nœud](#)

Créez une interface VLAN

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.
- Une interface de ligne réseau a été configurée sur le réseau et connectée au VM ou au nœud Linux. Vous connaissez le nom de l'interface de ligne réseau.
- Vous connaissez l'ID du VLAN que vous configurez.

Description de la tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs VLAN pour isoler le trafic client ou administrateur appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un ID numérique ou une balise. Par exemple, votre réseau peut utiliser le VLAN 100 pour le trafic FabricPool et le VLAN 200 pour une application d'archivage.

Vous pouvez utiliser Grid Manager pour créer des interfaces VLAN qui permettent aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID VLAN et sélectionnez des interfaces parent (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

1. Sélectionnez **CONFIGURATION réseau interfaces VLAN**.
2. Sélectionnez **Créer**.

Entrez les détails des interfaces VLAN

1. Spécifiez l'ID du VLAN de votre réseau. Vous pouvez entrer n'importe quelle valeur comprise entre 1 et 4094.

Les ID de 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 ayant le même ID ne peuvent pas partager la même interface sur un nœud.

Si vous spécifiez un ID déjà utilisé, un message s'affiche. Vous pouvez continuer à créer une autre interface VLAN pour le même ID VLAN, ou sélectionner **Annuler**, puis modifier l'ID existant.

2. Vous pouvez également saisir une brève description de l'interface VLAN.

VLAN details

VLAN ID ?

Description (optional) ?

60/64

Cancel Continue

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 du réseau d'administration (eth1) ne peuvent pas être utilisées en tant qu'interfaces parent et ne sont pas affichées.

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

- Passez en revue la configuration et apportez les modifications nécessaires.
 - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **entrer les détails du VLAN** en haut de la page.
 - Si vous devez modifier une interface parent, sélectionnez **Choisissez les interfaces parent** en haut de la page ou sélectionnez **Précédent**.
 - Si vous devez supprimer une interface parent, sélectionnez la corbeille .
- Sélectionnez **Enregistrer**.
- Attendez jusqu'à 5 minutes que la nouvelle interface apparaisse comme une sélection sur la page groupes haute disponibilité et qu'elle soit répertoriée dans la table **interfaces réseau** pour le nœud (**NOEUDS parent interface noeud Network**).

Modifiez une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID ou la description du VLAN.
- Ajouter ou supprimer des interfaces parent.

Par exemple, vous pouvez vouloir supprimer une interface parent d'une interface VLAN si vous envisagez de désaffecter le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID de VLAN si l'interface VLAN est utilisée dans un groupe haute disponibilité.

- Vous ne pouvez pas supprimer une interface parent si cette interface parent est utilisée dans un groupe haute disponibilité.

Par exemple, supposons que le VLAN 200 soit connecté aux interfaces parents des nœuds A et B. Si un groupe HA utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parent non utilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parent utilisée pour le nœud A.

Étapes

1. Sélectionnez **CONFIGURATION réseau interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN que vous souhaitez 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. Éventuellement, cocher ou décocher les cases pour ajouter des interfaces parent ou supprimer les 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 que vous souhaitez 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.

Gérez les groupes haute disponibilité

Gestion des groupes haute disponibilité (HA) : présentation

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité. En cas de défaillance de l'interface active dans le groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail.

Qu'est-ce qu'un groupe haute disponibilité ?

Vous pouvez utiliser des groupes HA (haute disponibilité) pour assurer des connexions de données hautement disponibles pour les clients S3 et Swift, ou fournir des connexions extrêmement disponibles à Grid Manager et au tenant Manager.

Chaque groupe HA permet d'accéder aux services partagés sur les nœuds sélectionnés.

- Les groupes HAUTE DISPONIBILITÉ, incluant les nœuds de passerelle et les nœuds d'administration, ou les deux, fournissent des connexions de données hautement disponibles pour les clients S3 et Swift.
- Les groupes HAUTE DISPONIBILITÉ comprenant uniquement des nœuds d'administration fournissent des connexions hautement disponibles au Grid Manager et au tenant Manager.
- Un groupe haute disponibilité comprenant uniquement des appliances SG100 ou SG1000 et des nœuds logiciels VMware peut offrir des connexions hautement disponibles pour [Locataires S3 avec S3 Select](#). Les groupes HAUTE DISPONIBILITÉ sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Comment créer un groupe haute disponibilité ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface réseau client (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.



Vous ne pouvez pas ajouter une interface à un groupe haute disponibilité si cette adresse IP est attribuée par DHCP.

2. Vous spécifiez une interface à utiliser comme interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous affectez une à 10 adresses IP virtuelles (VIP) au groupe. Les applications clients peuvent utiliser l'une de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, reportez-vous à la section [Configurez les groupes haute disponibilité](#).

Qu'est-ce que l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe haute disponibilité sont ajoutées à l'interface principale, qui est la première interface dans l'ordre prioritaire. Tant que l'interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n'importe quelle adresse VIP pour le groupe. C'est-à-dire, en fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, en fonctionnement normal, toute interface de priorité inférieure du groupe HA agit comme des interfaces de « sauvegarde ». Ces interfaces de sauvegarde ne sont pas utilisées sauf si l'interface principale (actuellement active) devient indisponible.

Afficher l'état actuel du groupe haute disponibilité d'un nœud

Pour vérifier si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **NOEUDS** *node*.

Si l'onglet **Présentation** inclut une entrée pour **groupes HA**, le nœud est affecté aux groupes HA répertoriés. La valeur après le nom du groupe est l'état actuel du nœud du groupe HA :

- **Actif** : le groupe HA est actuellement hébergé sur ce nœud.
- **Backup** : le groupe HA n'utilise pas ce nœud, c'est une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service haute disponibilité (obtenu par clé) a été arrêté manuellement.
- **Défaut** : 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 la défaillance du service CLB (obsolète) ou des services pour le Grid Manager ou le tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes aient peu d'impact et peuvent compter sur des comportements de tentatives normales pour poursuivre le fonctionnement.

Lorsqu'une panne est résolue et qu'une interface de priorité supérieure est à nouveau disponible, les adresses VIP sont automatiquement transférées vers l'interface de priorité la plus élevée disponible.

Comment sont utilisés les groupes haute disponibilité ?

Vous pouvez utiliser des groupes haute disponibilité pour fournir des connexions extrêmement disponibles à StorageGRID pour les données d'objet et pour les tâches d'administration.

- Un groupe haute disponibilité peut fournir des connexions administratives hautement disponibles vers le Grid Manager ou le tenant Manager.
- Un groupe haute disponibilité peut fournir des connexions de données extrêmement disponibles pour les clients S3 et Swift.
- Un groupe haute disponibilité ne contenant qu'une interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe haute disponibilité peut assurer la haute disponibilité uniquement si tous les nœuds du groupe fournissent les mêmes services. Lorsque vous créez un groupe haute disponibilité, ajoutez des interfaces à partir des types de nœuds qui fournissent les services requis.

- **Nœuds d'administration** : incluez le service Load Balancer et activez l'accès au Grid Manager ou au Gestionnaire de locataires.
- **Gateway Nodes** : inclut le service Load Balancer et le service CLB (obsolète).

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 ou Swift — Service Load Balancer	• 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	• Appareils SG100 ou SG1000 • Nœuds logiciels VMware Remarque : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas requis.
Accès client S3 ou Swift — service CLB Note: le service CLB est obsolète.	• Nœuds de passerelle

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.

Limites de l'utilisation de groupes HA avec le service CLB

La défaillance du service CLB ne déclenche pas de basculement au sein du groupe HA.

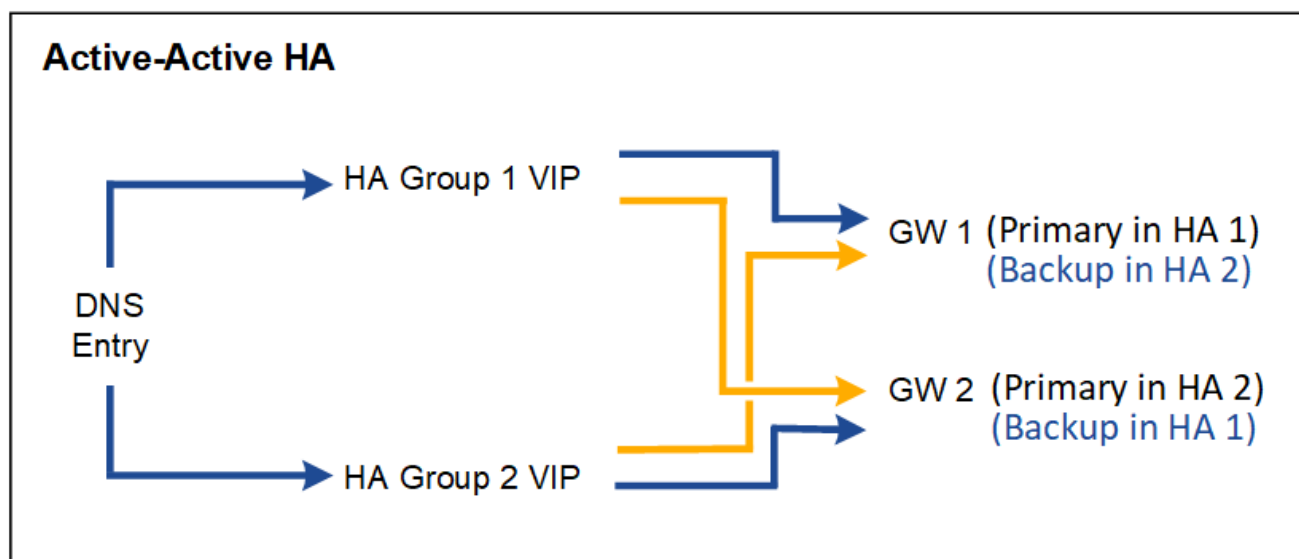
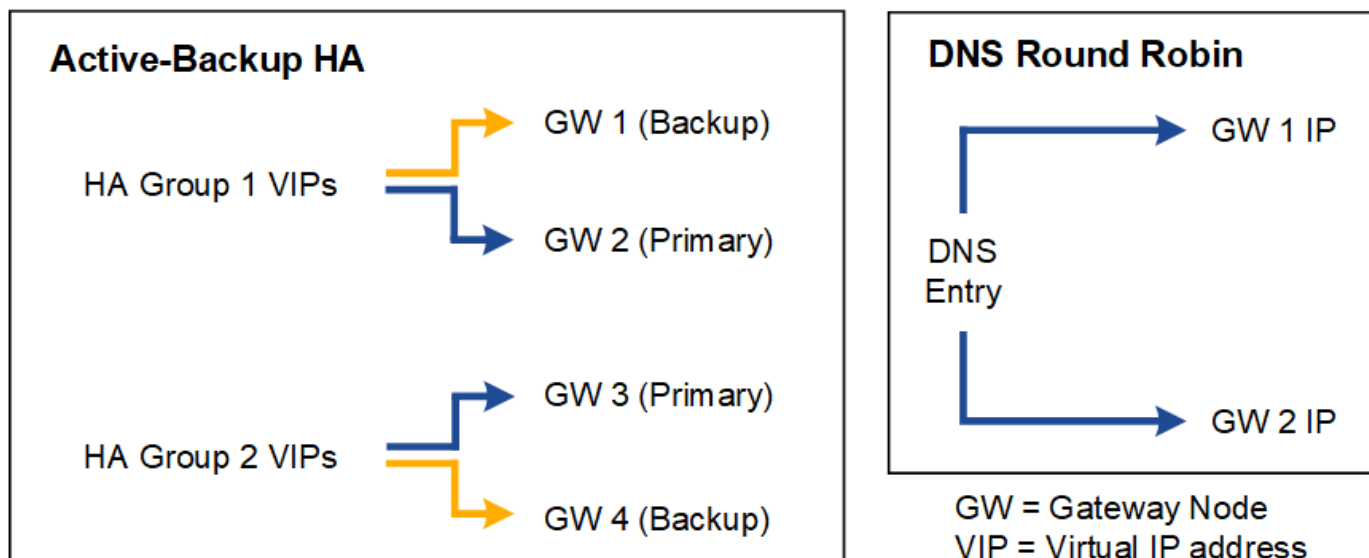


Le service CLB est obsolète.

Options de configuration pour les groupes haute disponibilité

Les schémas ci-dessous fournissent des exemples de différentes façons de configurer les groupes haute disponibilité. Chaque option présente des avantages et des inconvénients.

Dans les schémas, le bleu indique l'interface principale du groupe haute disponibilité et la jaune indique l'interface de sauvegarde du groupe haute disponibilité.



Le tableau récapitule les avantages de chaque configuration de haute disponibilité illustrée sur le schéma.

Configuration	Avantages	Inconvénients
Active-Backup HA	- Gérées par StorageGRID sans dépendances externes - Basculement rapide	Un seul nœud d'un groupe haute disponibilité est actif. Au moins un nœud par groupe haute disponibilité sera inactif.
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 les groupes haute disponibilité

Vous pouvez configurer des groupes haute disponibilité pour fournir un accès haute disponibilité aux services sur des nœuds d'administration ou de passerelle.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe haute disponibilité, vous avez créé cette interface. Voir [Configurez les interfaces VLAN](#).
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud d'un groupe haute disponibilité, vous avez créé l'interface :
 - **Red Hat Enterprise Linux ou CentOS (avant d'installer le nœud)** : [Créez des fichiers de configuration de nœud](#)
 - **Ubuntu ou Debian (avant d'installer le nœud)** : [Créez des fichiers de configuration de nœud](#)
 - **Linux (après l'installation du nœud)** : [Linux : ajoutez une jonction ou des interfaces d'accès à un nœud](#)
 - **VMware (après l'installation du nœud)** : [VMware : ajoutez du jonction ou des interfaces d'accès à un nœud](#)

Créez un groupe haute disponibilité

Lorsque vous créez un groupe haute disponibilité, vous sélectionnez une ou plusieurs interfaces et organisez-les par ordre de priorité. Vous affectez ensuite une ou plusieurs adresses VIP au groupe.

Pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe haute disponibilité, une interface doit être configurée pour inclure un nœud de passerelle. Un groupe haute disponibilité ne peut utiliser qu'une interface pour un nœud donné. Toutefois, les autres interfaces du même nœud peuvent être utilisées dans d'autres groupes haute disponibilité.

Accéder à l'assistant

1. Sélectionnez **CONFIGURATION réseau groupes haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe haute disponibilité

1. Indiquez un nom unique pour le groupe HA.

×

Create a high availability group

1 Enter details

2 Add interfaces

3 Prioritize interfaces

4 Enter IP addresses

Enter details for the HA group

HA group name

Description (optional)

- Si vous le souhaitez, entrez une description pour le groupe HA.
- Sélectionnez **Continuer**.

Ajouter des interfaces au groupe haute disponibilité

- 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.

Search...

Q

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

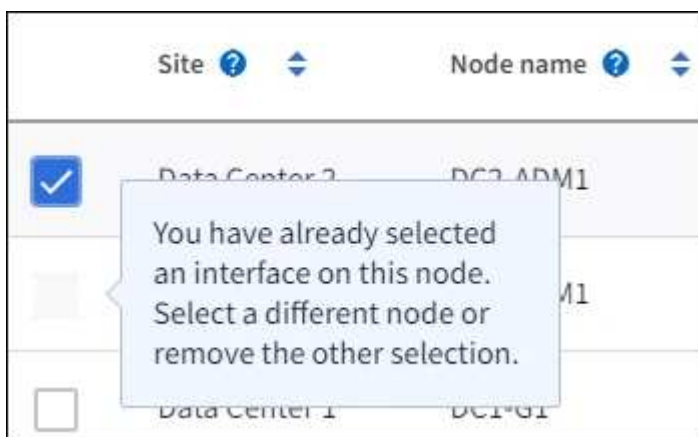
0 interfaces selected



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 HA est destiné à la protection HA du trafic client S3 ou Swift, sélectionnez les interfaces dans les nœuds d'administration, les nœuds de passerelle ou les deux.
- Si le groupe haute disponibilité est destiné à la protection haute disponibilité du service CLB obsolète, sélectionnez uniquement les interfaces sur les nœuds de passerelle.
- 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 HA des services du nœud d'administration. De même, un nœud d'administration de sauvegarde ne peut pas effectuer toutes les procédures de maintenance que le nœud d'administration principal peut fournir.
- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L'info-bulle fournit plus d'informations.



- Vous ne pouvez pas sélectionner une interface si sa valeur de sous-réseau ou sa passerelle 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

1. Déterminez l'interface principale et toutes les interfaces de sauvegarde (basculement) pour ce groupe haute disponibilité.

Faites glisser et déposez des lignes pour modifier les valeurs dans la colonne **ordre de priorité**.

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.

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 principale échoue, les adresses VIP passent à l'interface à la priorité la plus élevée qui est disponible. En cas d'échec de cette interface, les adresses VIP passent à l'interface de priorité supérieure suivante disponible, etc.

2. Sélectionnez **Continuer**.

Saisissez les adresses IP

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 des clients S3, Swift, d'administration ou de locataires accèdent à ces adresses VIP à partir d'un sous-réseau différent, saisissez l'adresse IP **Gateway**. L'adresse de la passerelle doit se trouver dans le sous-réseau VIP.

Les utilisateurs client et admin utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

- Entrez une ou plusieurs **adresses IP virtuelles** pour le groupe HA. Vous pouvez ajouter jusqu'à 10 adresses IP. Tous les VIP doivent être inclus dans le sous-réseau VIP.

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.



Attendez 15 minutes que les modifications d'un groupe haute disponibilité soient appliquées à tous les nœuds.

Étapes suivantes

Si vous utilisez ce groupe haute disponibilité pour équilibrer la charge, créez un terminal d'équilibreur de charge afin de déterminer le port et le protocole réseau, et de connecter tous les certificats requis. Voir [Configurer les terminaux de l'équilibreur de charge](#).

Modifiez un groupe haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour modifier son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous devrez peut-être modifier un groupe haute disponibilité si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans la procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **CONFIGURATION réseau groupes haute disponibilité**.

La page groupes haute disponibilité affiche tous les groupes haute disponibilité existants.

High availability groups

[Learn more about HA groups](#)

You can group the network interfaces of multiple Admin and Gateway Nodes into a high availability (HA) group. If the active interface in the group fails, a backup interface can manage the workload.

Each HA group provides access to the shared services on the selected nodes. Select Gateway Nodes, Admin Nodes, or both for load balancing. Select Admin Nodes for management services. All interfaces in a group must be in the same subnet. You assign one or more virtual IP addresses (VIPs) to each group. Clients use these VIPs to connect to StorageGRID.

You cannot select an interface if it has a DHCP-assigned IP address.

Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Create

Actions ▾

Search...

Q

Total HA groups count: 2

☐	Name ? ▴ ▾	Description ? ▴ ▾	Virtual IP address ? ▴ ▾	Interfaces (in priority order) ? ▴ ▾
☐	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
☐	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

← Previous 1 Next →

2. Cochez la case du groupe HA que vous souhaitez modifier.
3. Effectuez l'une des opérations suivantes, en fonction de ce que vous souhaitez mettre à jour :
 - Sélectionnez **actions Modifier l'adresse IP virtuelle** pour ajouter ou supprimer des adresses VIP.
 - Sélectionnez **actions Modifier le groupe HA** pour mettre à jour le nom ou la description du groupe, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou supprimer des adresses VIP.
4. Si vous avez sélectionné **Modifier l'adresse IP virtuelle** :
 - a. Mettre à jour les adresses IP virtuelles 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. Sélectionner ou désélectionner les cases à cocher 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 et déposer des lignes pour modifier l'ordre de priorité de l'interface principale et des interfaces de sauvegarde pour ce groupe haute disponibilité.
- d. Si vous le souhaitez, mettez à jour les adresses IP virtuelles.
- e. Sélectionnez **Enregistrer**, puis **Terminer**.



Attendez 15 minutes que les modifications d'un groupe haute disponibilité soient appliquées à tous les nœuds.

Supprimer un groupe haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes haute disponibilité (HA) à la fois. Toutefois, vous ne pouvez pas supprimer un groupe HA s'il est lié à un ou plusieurs terminaux d'équilibrage de la charge.

Pour éviter les interruptions de vos clients, mettez à jour les applications clients S3 ou Swift affectées avant de supprimer un groupe haute disponibilité. Mettre à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe haute disponibilité ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **CONFIGURATION réseau groupes haute disponibilité**.
2. Cochez la case correspondant à chaque groupe haute disponibilité à supprimer. Sélectionnez ensuite **actions Supprimer le groupe HA**.
3. 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

Gérer l'équilibrage de charge : présentation

Vous pouvez utiliser les fonctions d'équilibrage de charge StorageGRID pour gérer les workloads d'ingestion et de récupération à partir de clients S3 et Swift. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en distribuant les charges de travail et les connexions entre plusieurs nœuds de stockage.

Vous pouvez équilibrer la charge des workloads clients de l'une des manières suivantes :

- Utilisez le service Load Balancer, qui est installé sur les nœuds d'administration et les nœuds de passerelle. Le service Load Balancer assure l'équilibrage de la charge de couche 7 et effectue la résiliation TLS des requêtes client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage. Il s'agit du mécanisme d'équilibrage de charge recommandé.

Voir [Fonctionnement de l'équilibrage de la charge : service Load Balancer](#).

- Utilisez le service CLB (Connection Load Balancer) obsolète, qui est installé uniquement sur les nœuds de passerelle. Le service CLB assure l'équilibrage de charge de couche 4 et prend en charge les coûts de liaison.

Voir [Fonctionnement de l'équilibrage des charges - service CLB \(obsolète\)](#).

- Intégrez un équilibreur de charge tiers. Pour plus d'informations, contactez votre ingénieur commercial NetApp.

Fonctionnement de l'équilibrage de la charge : service Load Balancer

Le service Load Balancer distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Pour activer l'équilibrage de charge, vous devez configurer les nœuds finaux de l'équilibreur de charge à l'aide de Grid Manager.

Vous pouvez configurer les nœuds finaux de l'équilibreur de charge uniquement pour les nœuds d'administration ou les nœuds de passerelle, car ces types de nœuds contiennent le service Load Balancer. Vous ne pouvez pas configurer de nœuds finaux pour les nœuds de stockage ou les nœuds d'archivage.

Chaque point final de l'équilibreur de charge spécifie un port, un protocole réseau (HTTP ou HTTPS), un type de client (S3 ou Swift) et un mode de liaison. Les terminaux HTTPS requièrent un certificat de serveur. Les modes de liaison vous permettent de limiter l'accessibilité des ports de point final à :

- Adresses IP virtuelles (VIP) de groupes haute disponibilité (HA) spécifiques
- Interfaces réseau spécifiques de nœuds d'administration et de passerelle spécifiques

Considérations relatives aux ports

Les clients peuvent accéder à tous les terminaux que vous configurez sur n'importe quel nœud exécutant le service Load Balancer, à deux exceptions près : les ports 80 et 443 sont réservés aux nœuds d'administration. Les terminaux configurés sur ces ports prennent donc en charge les opérations d'équilibrage de la charge uniquement sur les nœuds de passerelle.

Si vous avez mappé de nouveau des ports, vous ne pouvez pas utiliser les mêmes ports pour configurer les points finaux de l'équilibreur de charge. Vous pouvez créer des nœuds finaux à l'aide de ports remappés, mais ces nœuds finaux seront remappés vers les ports et le service CLB d'origine, et non le service Load Balancer. Suivez les étapes de la section [Supprimer les mappages de port](#).



Le service CLB est obsolète.

Disponibilité du processeur

Le service Load Balancer sur chaque nœud d'administration et chaque nœud de passerelle fonctionne de manière indépendante lors du transfert du trafic S3 ou Swift vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure. Les informations de charge de l'UC du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids de base minimale, même si un nœud indique une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service Load Balancer.

Configurer les terminaux de l'équilibreur de charge

Les terminaux d'équilibrage de la charge déterminent les ports et les protocoles réseau que les clients S3 et Swift peuvent utiliser pour la connexion à l'équilibreur de charge StorageGRID sur les nœuds de passerelle et d'administration.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.
- Si vous avez précédemment mappé à nouveau un port que vous souhaitez utiliser pour le nœud final de l'équilibreur de charge, vous avez [retirez le schéma de câblage des ports - effectué](#).
- Vous avez créé tous les groupes à haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HAUTE DISPONIBILITÉ sont recommandés, mais pas obligatoires. Voir [Gérez les groupes haute disponibilité](#).
- Si le point final de l'équilibreur de charge est utilisé par [Locataires S3 pour S3 Select](#), Il ne doit pas utiliser les adresses IP ou FQDN de tout nœud bare-Metal. Seuls les appliances SG100 ou SG1000 et les nœuds logiciels VMware sont autorisés pour les terminaux d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir [Configurez les interfaces VLAN](#).
- Si vous créez un nœud final HTTPS (recommandé), vous disposez des informations relatives au certificat de serveur.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

- Pour télécharger un certificat, vous avez besoin du certificat de serveur, de la clé privée de certificat et, éventuellement, d'un bundle CA.
- Pour générer un certificat, vous devez disposer de tous les noms de domaine et adresses IP que les clients S3 ou Swift utiliseront pour accéder au terminal. Vous devez également connaître le sujet (Nom unique).
- Si vous souhaitez utiliser le certificat API StorageGRID S3 et Swift (qui peut également être utilisé pour les connexions directement aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir [Configurez les certificats API S3 et Swift](#).

Le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et 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. Voir [Configurez les noms de domaine de terminaux API S3](#).

Créer un nœud final d'équilibreur de charge

Chaque point final de l'équilibreur de charge spécifie un port, un type de client (S3 ou Swift) et un protocole réseau (HTTP ou HTTPS).

Accéder à l'assistant

1. Sélectionnez **CONFIGURATION réseau points d'extrémité de l'équilibreur de charge**.

2. Sélectionnez **Créer**.

Saisissez les détails du point final

1. Saisissez les détails du noeud final.

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name

Port

Enter an unused port or accept the suggested port.

10443

Client type

Select the type of client application that will use this endpoint.

☒ S3

☐ Swift

Network protocol

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended)

☒ HTTP

Cancel

Continue

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	Les ports clients utilisent pour se connecter au service Load Balancer sur les nœuds d'administration et les nœuds de passerelle. Acceptez le numéro de port suggéré ou entrez tout port externe qui n'est pas utilisé par un autre service de grille. Entrez une valeur comprise entre 1 et 65535. Si vous saisissez 80 ou 443, le nœud final est configuré uniquement sur les nœuds de passerelle. Ces ports sont réservés sur des nœuds d'administration. Voir la Instructions de mise en réseau pour plus d'informations sur les ports externes.
Type de client	Type d'application client qui utilisera ce nœud final, S3 ou Swift .
Protocole réseau	Protocole réseau utilisé par les clients lors de la connexion à ce nœud final. • Sélectionnez HTTPS pour la communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le nœud final. • Sélectionnez HTTP pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille autre que la production.

2. Sélectionnez **Continuer**.

Sélectionnez le mode de reliure

1. Sélectionnez un mode de liaison pour le nœud final afin de contrôler l'accès au nœud final.

Option	Description
Global (par défaut)	Les clients peuvent accéder au nœud final à l'aide d'un nom de domaine complet (FQDN), de l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration, ou de l'adresse IP virtuelle d'un groupe HA sur n'importe quel réseau. Utilisez le paramètre Global (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Interfaces de nœuds	Les clients doivent utiliser l'adresse IP d'un nœud et d'une interface réseau sélectionnés pour accéder à ce nœud final.

Option	Description
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle d'un groupe haute disponibilité pour accéder à ce noeud final. Les terminaux peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas. Les noeuds finaux avec ce mode peuvent tous utiliser le même numéro de port tant que les interfaces sélectionnées pour les noeuds finaux ne se chevauchent pas.



Si vous utilisez le même port pour plusieurs noeuds finaux, un noeud final utilisant le mode **IP virtuelles de groupes HA** remplace un noeud final en utilisant le mode **interfaces Node**, qui remplace un noeud final en utilisant le mode **Global**.

- Si vous avez sélectionné **Node interfaces**, sélectionnez une ou plusieurs interfaces de nœud pour chaque noeud d'administration ou nœud de passerelle que vous souhaitez associer à ce noeud final.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global
 ☒ Node interfaces
 ☐ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

?

Total interface count: 3

☐	Node ?	Node interface ?	Site ?	IP address ?	Node type ?
☐	DC1-ADM1	eth0 ?	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
☐	DC1-ADM1	eth1 ?	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
☐	DC1-ADM1	eth2 ?	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

- Si vous avez sélectionné **IP virtuelles de groupes HA**, sélectionnez un ou plusieurs groupes HA.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☐ Node interfaces ☒ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...				Total interface count: 2
☐	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
☐	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
☐	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. Si vous créez un noeud final **HTTP**, vous n'avez pas besoin d'attacher 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

1. Si vous créez un noeud final **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au noeud final.

Le certificat sécurise les connexions entre les clients S3 et Swift et le service Load Balancer sur les nœuds d'administration ou de passerelle.

- **Télécharger le certificat.** Sélectionnez cette option si vous avez des certificats personnalisés à télécharger.
- **Générer un certificat.** Sélectionnez cette option si vous avez les valeurs nécessaires pour générer un certificat personnalisé.
- **Utilisez le certificat StorageGRID S3 et Swift.** Sélectionnez cette option pour utiliser le certificat d'API S3 et Swift global, qui peut également être utilisé pour les connexions directement aux nœuds de stockage.

Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 et Swift par défaut, signé par l'autorité de certification de la grille, par un certificat personnalisé signé par une autorité de certification externe. Voir [Configurez les certificats API S3 et Swift](#).

2. Si vous n'utilisez pas le certificat StorageGRID S3 et Swift, téléchargez ou générez le certificat.

Télécharger le certificat

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé dans le codage PEM.
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (.key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Créer**. + le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 et Swift et le terminal.

Générez un certificat

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

- **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés 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.
- **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides**: Nombre de jours après la création que le certificat expire.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Créer**.

Le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 et Swift et ce terminal.

après que vous avez terminé

1. Si vous utilisez un système de noms de domaine (DNS), assurez-vous que le DNS inclut un enregistrement pour associer le nom de domaine complet 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 connecteront au service StorageGRID Load Balancer à l'aide de l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point final requis, y compris les noms de caractères génériques.

2. Fournissez aux clients S3 et Swift les informations nécessaires pour se connecter au terminal :

- Numéro de port
- Nom de domaine ou adresse IP complet
- Tous les détails de certificat requis

Afficher et modifier les points finaux de l'équilibreur de charge

Vous pouvez afficher les détails des noeuds finaux existants de l'équilibreur de charge, y compris les métadonnées de certificat d'un noeud final sécurisé. Vous pouvez également modifier le nom d'un noeud final ou le mode de liaison et mettre à jour tous les certificats associés.

Vous ne pouvez pas modifier le type de service (S3 ou Swift), le port ou le protocole (HTTP ou HTTPS).

- Pour afficher les informations de base de tous les noeuds finaux de l'équilibreur de charge, consultez le tableau de la page noeuds finaux de l'équilibreur de charge.

Create Actions Search... Total endpoints count: 1					
☐	Name ?	Port ?	Network protocol ?	Binding mode ?	Certificate expiration ?
☐	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022

- 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.

FabricPool endpoint 

Port:10443

Client type:S3

Network protocol:HTTPS

Binding mode:Global

Endpoint ID:c2b6feb3-c567-449d-b717-4fed98c4a411

Remove

Binding Mode

Certificate

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 de l'équilibreur de charge ou la page de détails d'un noeud final spécifique.



Après avoir modifié un noeud final, vous devrez peut-être attendre jusqu'à 15 minutes que vos modifications soient appliquées à tous les noeuds.

Tâche	Menu actions	Page de détails
Modifier le nom du point final	a. Cochez la case correspondant au 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.

Tâche	Menu actions	Page de détails
Modifier le mode de liaison du point final	a. Cochez la case correspondant au 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 correspondant au point final. b. Sélectionnez actions Modifier le certificat de point final . c. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat Global S3 et Swift, si nécessaire. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet certificat . c. Sélectionnez Modifier le certificat . d. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat Global S3 et Swift, si nécessaire. e. Sélectionnez Enregistrer les modifications .

Supprimez les points finaux de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs noeuds finaux à l'aide du menu **actions**, ou vous pouvez supprimer un seul noeud final de la page de détails.



Pour éviter toute interruption de vos clients, mettez à jour les applications client S3 ou Swift affectées avant de supprimer un terminal d'équilibrage de charge. Mettez à jour chaque client pour vous connecter à l'aide d'un port attribué à un autre noeud final de l'équilibreur de charge. Assurez-vous également de mettre à jour les informations de certificat requises.

- Pour supprimer un ou plusieurs noeuds finaux :
 - Dans la page équilibreur de charge, cochez la case pour chaque noeud final que vous souhaitez supprimer.
 - Sélectionnez **actions Supprimer**.
 - Sélectionnez **OK**.
- Pour supprimer un noeud final de la page de détails :
 - À partir de la page équilibreur de charge, sélectionnez le nom du noeud final.
 - Sélectionnez **Supprimer** sur la page de détails.
 - Sélectionnez **OK**.

Fonctionnement de l'équilibrage des charges - service CLB (obsolète)

Le service Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète.

Le service Load Balancer est désormais le mécanisme d'équilibrage de charge recommandé.

Le service CLB utilise l'équilibrage de charge de couche 4 pour distribuer les connexions réseau TCP entrantes des applications clientes vers le nœud de stockage optimal en fonction de la disponibilité, de la charge système et du coût de liaison configuré par l'administrateur. Lorsque le nœud de stockage optimal est choisi, le service CLB établit une connexion réseau bidirectionnelle et transfère le trafic vers et depuis le nœud choisi. Le CLB ne prend pas en compte la configuration du réseau Grid lors de la direction des connexions réseau entrantes.

Pour afficher des informations sur le service CLB, sélectionnez **SUPPORT Outils topologie de grille**, puis développez un nœud de passerelle jusqu'à ce que vous puissiez sélectionner **CLB** et les options ci-dessous.

The screenshot shows the 'Grid Topology' interface. On the left, a tree view under 'StorageGRID Webscale Deployment' shows 'Data Center 1' expanded, with 'DC1-G1-98-161' selected. This node contains 'SSM', 'CLB', 'HTTP', 'Events', and 'Resources'. On the right, the 'Overview' tab is active, displaying 'Overview: Summary - DC1-G1-98-161' with an update timestamp of '2015-10-27 16:23:33 PDT'. Below this, a 'Storage Capacity' section contains a table with the following data:

Storage Nodes Installed:	N/A	
Storage Nodes Readable:	N/A	
Storage Nodes Writable:	N/A	
Installed Storage Capacity:	N/A	
Used Storage Capacity:	N/A	
Used Storage Capacity for Data:	N/A	
Used Storage Capacity for Metadata:	N/A	
Usable Storage Capacity:	N/A	

Si vous choisissez d'utiliser le service CLB, vous devriez envisager de configurer les coûts de liaison pour votre système StorageGRID.

- [Quels sont les coûts de liaison](#)
- [Mettre à jour les coûts des liens](#)

Configurez les noms de domaine de terminaux API S3

Pour prendre en charge les demandes de type hébergement virtuel S3, vous devez utiliser Grid Manager pour configurer la liste des noms de domaine de points de terminaison auxquels les clients S3 se connectent.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez confirmé qu'une mise à niveau de la grille n'est pas en cours.



Ne modifiez pas la configuration du nom de domaine lorsqu'une mise à niveau de la 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.
- Vérifiez que le certificat utilisé par le client pour les connexions HTTPS à StorageGRID est signé pour tous les noms de domaine requis par le client.

Par exemple, si le noeud final est `s3.company.com`, Vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` Nom de l'alternative (SAN) de l'objet générique du noeud final et du noeud final : `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Inclure les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et s'assurer que les enregistrements référencent tous les noms de domaine de point final requis, y compris les noms de caractères 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 noeud final de l'équilibreur de charge peut être configuré pour reconnaître différents noms de domaine de point final.
- Les clients qui se connectent à un terminal d'équilibreur de charge, directement à un nœud de stockage ou directement au service CLB obsolète sur un nœud de passerelle peuvent personnaliser le certificat API S3 et Swift global pour inclure tous les noms de domaine de terminal requis.

Étapes

1. Sélectionnez **CONFIGURATION réseau noms de domaine**.

La page noms de domaine de point final s'affiche.

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: `s3.example.com`, `s3.example.co.uk`, `s3-east.example.com`

Endpoint 1	s3.example.com	✕
Endpoint 2		+ ✕

2. Entrez la liste des noms de domaine de points de terminaison de l'API S3 dans les champs **Endpoint**. Utilisez le **+** pour ajouter des champs supplémentaires.

Si cette liste est vide, la prise en charge des demandes de type hébergement virtuel S3 est désactivée.

3. Sélectionnez **Enregistrer**.

4. Assurez-vous que les certificats de serveur utilisés par les clients correspondent aux noms de domaine de noeud final requis.
 - Si les clients se connectent à un noeud final de l'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'équilibreur de charge utilisant le certificat API global S3 et Swift, directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, mettez à jour le certificat API S3 et Swift global.
5. Ajoutez les enregistrements DNS requis pour vous assurer que les demandes de nom de domaine de point final peuvent être résolues.

Résultat

Maintenant, lorsque les clients utilisent le noeud final `bucket.s3.company.com`, Le serveur DNS résout le noeud final correct et le certificat authentifie le noeud final comme prévu.

Informations associées

- [Utilisation de S3](#)
- [Afficher les adresses IP](#)
- [Configurez les groupes haute disponibilité](#)
- [Configurez les certificats API S3 et Swift](#)
- [Configurer les terminaux de l'équilibreur de charge](#)

Activez HTTP pour les communications client

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions aux nœuds de stockage ou au service CLB obsolète sur les nœuds de passerelle. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille autre que la production.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Cette tâche doit être effectuée uniquement si les clients S3 et Swift doivent établir des connexions HTTP directement vers les nœuds de stockage ou vers le service CLB obsolète sur les nœuds de passerelle.

Il n'est pas nécessaire d'effectuer cette tâche pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (parce que vous pouvez configurer chaque noeud final Load Balancer pour utiliser HTTP ou HTTPS). Pour plus d'informations, reportez-vous aux informations sur la configuration des noeuds finaux de l'équilibreur de charge.

Voir [Résumé : adresses IP et ports pour les connexions client](#) Pour découvrir les ports que les clients S3 et Swift utilisent lors de la connexion aux nœuds de stockage ou au service CLB obsolète via HTTP ou HTTPS



Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options réseau, cochez la case **Activer la connexion HTTP**.

Network Options



3. Sélectionnez **Enregistrer**.

Informations associées

- [Configurer les terminaux de l'équilibreur de charge](#)
- [Utilisation de S3](#)
- [Utiliser Swift](#)

Contrôler les opérations client autorisées

Vous pouvez sélectionner l'option empêcher la grille de modification du client pour refuser des opérations client HTTP spécifiques.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option empêcher la modification du client est sélectionnée, les demandes suivantes sont refusées :

• API REST S3

- Supprimer les demandes de compartiment
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3



Ce paramètre ne s'applique pas aux compartiments avec la gestion des versions activée. Le contrôle de version empêche déjà les modifications des données d'objet, des métadonnées définies par l'utilisateur et du balisage d'objets.

• API REST Swift

- Supprimer les demandes de conteneur
- Demande de modifier tout objet existant. Par exemple, les opérations suivantes sont refusées : remplacement, suppression, mise à jour des métadonnées, etc.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options réseau, cochez la case **empêcher la modification du client**.

Network Options

Prevent Client Modification ☒

Enable HTTP Connection ☐

Network Transfer Encryption ☐ AES128-SHA ☒ AES256-SHA

3. Sélectionnez **Enregistrer**.

Gestion des réseaux et des connexions

Instructions pour les réseaux StorageGRID

Vous pouvez utiliser le Gestionnaire de grille pour configurer et gérer les réseaux et les connexions StorageGRID.

Voir [Configurez les connexions des clients S3 et Swift](#) Pour apprendre à connecter des clients S3 ou Swift.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, reportez-vous à la section [Instructions de mise en réseau](#).

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour l'ensemble du trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux.

Réseau d'administration

Facultatif. Le réseau d'administration est généralement utilisé pour l'administration et la maintenance du système. Il peut également être utilisé pour l'accès au protocole client. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir l'accès aux applications client S3 et Swift, de sorte que le réseau Grid puisse être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Directives

- Chaque nœud de grid StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est attribué.
- Un nœud de grid ne peut pas avoir plusieurs interfaces 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
Client (facultatif)	eth2

- Si le nœud est connecté à une appliance StorageGRID, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, reportez-vous aux instructions d'installation de votre appareil.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client n'est opérationnel qu'après que le nœud de la grille ait rejoint la grille
- Le réseau Admin peut être configuré pendant le déploiement du nœud grid pour permettre l'accès à l'interface utilisateur d'installation avant que la grille soit entièrement installée.

Interfaces en option

Vous pouvez également ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pouvez ajouter une interface de ligne réseau à un nœud d'administration ou de passerelle pour que vous puissiez utiliser [Interfaces VLAN](#) pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser dans un [Groupe haute disponibilité \(HA\)](#).

Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :

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

Afficher les adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud grid dans votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud grid en ligne de commande et effectuer diverses procédures de maintenance.

Ce dont vous avez besoin

Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

Description de la tâche

Pour plus d'informations sur la modification des adresses IP, reportez-vous à la section [Récupérer et entretenir](#).

Étapes

- 1. Sélectionnez **NOEUDS *grid noeud* Présentation**.
- 2. Sélectionnez **Afficher plus** à droite du titre des adresses IP.

Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.

DC2-SGA-010-096-106-021 (Storage Node) [✕](#)

OverviewHardwareNetworkStorageObjectsILMTasks

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.

204

Chiffrement pris en charge pour les connexions TLS sortantes

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (transport Layer Security) avec les systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Versions supportées de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Les chiffrements TLS qui sont pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour assurer la compatibilité avec une gamme de systèmes externes. La liste est plus grande que la liste des chiffrements pris en charge pour une utilisation avec les applications client S3 ou Swift.



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 en StorageGRID. Contactez votre ingénieur commercial NetApp pour toute demande spécifique concernant ces paramètres.

Suites de chiffrement TLS 1.2 prises en charge

Les suites de chiffrement TLS 1.2 suivantes sont prises en charge :

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Suites de chiffrement TLS 1.3 prises en charge

Les suites de chiffrement TLS 1.3 suivantes sont prises en charge :

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Modifiez le chiffrement du transfert réseau

Le système StorageGRID utilise TLS (transport Layer Security) pour protéger le trafic de contrôle interne entre les nœuds de la grille. L'option Network Transfer Encryption définit l'algorithme utilisé par TLS pour chiffrer le trafic de contrôle entre les nœuds de la grille. Ce paramètre n'affecte pas le chiffrement des données.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, le chiffrement de transfert réseau utilise l'algorithme AES256-SHA. Le trafic de contrôle peut également être crypté à l'aide de l'algorithme AES128-SHA.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options réseau, définissez cryptage de transfert réseau sur **AES128-SHA** ou **AES256-SHA** (par défaut).

Network Options



3. Sélectionnez **Enregistrer**.

Gérer les stratégies de classification du trafic

Gérer les stratégies de classification du trafic

Pour améliorer vos offres de qualité de service (QoS), vous pouvez créer des stratégies de classification du trafic afin d'identifier et de surveiller différents types de trafic réseau. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Les règles de classification du trafic sont appliquées aux terminaux du service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des stratégies de classification de trafic, vous devez avoir déjà créé des points d'extrémité d'équilibreur de charge.

Règles de correspondance

Chaque règle de classification de trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Locataires
- Sous-réseaux (sous-réseaux IPv4 contenant le client)
- Terminaux (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 définir des limites pour une stratégie en fonction des paramètres suivants :

- Bande passante agrégée dans
- Bande passante de l'agrégat sortie
- Demandes de lecture simultanée
- Demandes d'écriture simultanées
- Bande passante par demande dans
- Bande passante à la demande
- Taux de demande de lecture
- Taux de demandes d'écriture

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 simultanément les deux types de bande passante. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante globale ou par requête, les demandes sont envoyées vers l'intérieur ou vers l'extérieur au débit défini. StorageGRID ne peut appliquer qu'une seule vitesse. La correspondance des règles la plus spécifique, par type de contrôleur, est donc la plus appliquée. Pour tous les autres types de limite, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse lente de 503 pour les demandes dépassant toute limite de stratégie correspondante.

Dans Grid Manager, vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Utilisez les stratégies de classification du trafic avec les contrats de niveau de service

Vous pouvez utiliser des règles de classification du trafic en association avec les limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des spécificités en matière de capacité, de protection des données et de performances.

Les limites de classification du trafic sont mises en œuvre 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.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des règles de classification du trafic pour atteindre les objectifs de performances de chaque niveau de contrat de niveau de service.

Niveau de service	Puissance	La protection des données	Performance	Le coût
Or	1 po de stockage autorisé	Règle ILM de 3 copies	25 000 demandes/s Bande passante de 5 Go/s (40 Gbit/s)	par mois
Argent	Stockage de 250 To autorisé	Règle ILM 2 copies	10 000 demandes/s Bande passante de 1.25 Go/s (10 Gbit/s)	\$\$ par mois
Bronze	Stockage de 100 To autorisé	Règle ILM 2 copies	5 000 demandes/s Bande passante de 1 Go/s (8 Gbit/s)	\$ par mois

Créer des stratégies de classification du trafic

Vous créez des règles de classification du trafic pour surveiller et limiter, éventuellement, le trafic réseau par compartiment, locataire, sous-réseau IP ou point de terminaison d'équilibrage de la charge. 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.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.
- Vous avez créé tous les noeuds finaux de l'équilibreur de charge que vous souhaitez associer.
- Vous avez créé les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **CONFIGURATION réseau classification du trafic**.

La page règles de classification du trafic s'affiche.

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
No policies found.		

2. Sélectionnez **Créer**.

La boîte de dialogue Créer une stratégie de classification de trafic s'affiche.

Create Traffic Classification Policy

Policy

Name 

Description

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create

 Edit

 Remove

Type	Inverse Match	Match Value
No matching rules found.		

Limits (Optional)

+ Create

 Edit

 Remove

Type	Value	Units
No limits found.		

Cancel

Save

3. Dans le champ **Nom**, entrez un nom pour la stratégie.

Entrez un nom descriptif pour reconnaître la stratégie.

4. Vous pouvez également ajouter une description de la stratégie dans le champ **Description**.

Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

5. Créer une ou plusieurs règles de correspondance pour la règle.

Les règles de correspondance contrôlent les entités qui seront affectées par cette politique de classification du trafic. Par exemple, sélectionnez tenant si vous souhaitez que cette stratégie s'applique au trafic réseau d'un locataire spécifique. Ou sélectionnez point final si vous souhaitez que cette stratégie s'applique au trafic réseau sur un point final d'équilibreur de charge spécifique.

- a. Sélectionnez **Créer** dans la section **règles de correspondance**.

La boîte de dialogue Créer une règle de correspondance s'affiche.

209

Create Matching Rule

Matching Rules

Type  -- Choose One -- 

Match Value  Choose type before providing match value

Inverse Match  ☐

- b. Dans la liste déroulante **Type**, sélectionnez le type d'entité à inclure dans la règle correspondante.
- c. Dans le champ **valeur de correspondance**, entrez une valeur de correspondance basée sur le type d'entité que vous avez choisi.

- Compartiment : entrez un nom de compartiment.
- Regex du compartiment : saisissez une expression régulière qui sera utilisée pour correspondre à un ensemble de noms de compartiment.

L'expression régulière n'est pas ancrée. Utilisez l'ancre ^ pour faire correspondre au début du nom du compartiment, et utilisez l'ancre \$ pour correspondre à la fin du nom.

- CIDR : saisissez un sous-réseau IPv4, en notation CIDR, qui correspond au sous-réseau souhaité.
 - Noeud final : sélectionnez un noeud final dans la liste des noeuds finaux existants. Il s'agit des noeuds finaux de l'équilibreur de charge que vous avez définis sur la page noeuds finaux de l'équilibreur de charge. Voir [Configurer les terminaux de l'équilibreur de charge](#).
 - Locataire : sélectionnez un locataire dans la liste des locataires existants. La correspondance établie entre les locataires dépend de la propriété du compartiment utilisé. L'accès anonyme à un compartiment correspond au locataire qui détient le compartiment.
- d. Si vous souhaitez faire correspondre tout le trafic réseau *exception* trafic correspondant au type et à la valeur de correspondance que vous venez de définir, cochez la case **inverse**. Sinon, ne cochez pas la case.

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 **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.

- e. Sélectionnez **appliquer**.

La règle est créée et répertoriée dans le tableau règles de correspondance.

+ Create
Edit
Remove

Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

Type	Value	Type	Units
No limits found.			

Cancel
Save

a. Répétez ces étapes pour chaque règle que vous souhaitez créer pour la règle.

 Le trafic correspondant à n'importe quelle règle est géré par la règle.

6. Vous avez la possibilité de créer des limites pour la règle.

 Même si vous ne créez pas de limites, StorageGRID collecte des mesures pour vous permettre de surveiller le trafic réseau qui correspond à la stratégie.

a. Sélectionnez **Créer** dans la section **limites**.

La boîte de dialogue Créer limite s'affiche.

Create Limit

Limits (Optional)

Type
?
-- Choose One --

Aggregate rate limits in use. Per-request rate limits are not available.
?

Value
?

Cancel
Apply

b. Dans la liste déroulante **Type**, sélectionnez le type de limite que vous souhaitez appliquer à la stratégie.

Dans la liste suivante, **in** désigne le trafic des clients S3 ou Swift vers l'équilibreur de charge

StorageGRID et **OUT** désigne le trafic de l'équilibreur de charge vers les clients S3 ou Swift.

- Bande passante agrégée dans
- Bande passante de l'agrégat sortie
- Demandes de lecture simultanée
- Demandes d'écriture simultanées
- Bande passante par demande dans
- Bande passante à la demande
- Taux de demande de lecture
- Taux de demandes d'écriture



Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter simultanément les deux types de bande passante. 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 des correspondances « meilleures » 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

c. Dans le champ **valeur**, entrez une valeur numérique pour le type de limite que vous avez choisi.

Les unités attendues s'affichent lorsque vous sélectionnez une limite.

d. Sélectionnez **appliquer**.

La limite est créée et est répertoriée dans le tableau limites.

+ Create
Edit
Remove

Type	Inverse Match	Match Value
☒ Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

Type	Value	Units
☒ Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel
Save

e. Répétez ces étapes pour chaque limite que vous souhaitez ajouter à la stratégie.

Par exemple, si vous souhaitez créer une limite de bande passante de 40 Gbits/s pour un niveau de contrat de niveau de service, créez une limite de bande passante agrégée et une limite de bande passante agrégée OUT et définissez chacune sur 40 Gbits/s.



Pour convertir les mégaoctets par seconde en gigabits par seconde, multipliez par huit. Par exemple, 125 Mo/s équivaut à 1,000 Mbit/s ou 1 Gbit/s.

7. Lorsque vous avez terminé de créer des règles et des limites, sélectionnez **Enregistrer**.

La police est enregistrée et est répertoriée dans le tableau règles de classification du trafic.

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-7665bddc894b

Displaying 2 traffic classification policies.

Le trafic client S3 et Swift 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. Voir [Afficher les données de trafic réseau](#).

Modifier une règle de classification de trafic

Vous pouvez modifier une stratégie de classification de trafic pour modifier son nom ou

sa description, ou pour créer, modifier ou supprimer des règles ou des limites de la stratégie.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION réseau classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans 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.

2. Sélectionnez le bouton radio à gauche de la police que vous souhaitez modifier.
3. Sélectionnez **Modifier**.

La boîte de dialogue Modifier la stratégie de classification de trafic s'affiche.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name 

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

 Create

 Edit

 Remove

	Type	Inverse Match	Match Value
☒	CIDR		10.10.152.0/24

Displaying 1 matching rule.

Limits (Optional)

 Create

 Edit

 Remove

	Type	Value	Units

No limits found.

Cancel

Save

4. Créez, modifiez ou supprimez des règles et des limites de correspondance selon les besoins.
 - a. Pour créer une règle ou une limite de correspondance, sélectionnez **Créer** et suivez les instructions pour créer une règle ou créer une limite.
 - b. Pour modifier une règle ou une limite de correspondance, sélectionnez le bouton radio de la règle ou de la limite, sélectionnez **Modifier** dans la section **règles de mise en correspondance** ou **limites** et suivez les instructions pour créer une règle ou créer une limite.
 - c. Pour supprimer une règle ou une limite correspondante, sélectionnez le bouton radio de la règle ou de la limite, puis sélectionnez **Supprimer**. Sélectionnez ensuite **OK** pour confirmer que vous souhaitez supprimer la règle ou la limite.
5. Lorsque vous avez terminé de créer ou de modifier une règle ou une limite, sélectionnez **appliquer**.
6. Lorsque vous avez terminé de modifier la stratégie, sélectionnez **Enregistrer**.

Les modifications apportées à la stratégie sont enregistrées et le trafic réseau est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Supprimer une règle de classification du trafic

Si vous n'avez plus besoin d'une règle de classification du trafic, vous pouvez la supprimer.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION réseau classification du trafic**.

La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans 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.			

2. Sélectionnez le bouton radio à gauche de la police que vous souhaitez supprimer.
3. Sélectionnez **Supprimer**.

Une boîte de dialogue Avertissement s'affiche.

 **Warning**

Delete Policy

Are you sure you want to delete the policy "Fabric Pools"?

Cancel OK

4. Sélectionnez **OK** pour confirmer que vous souhaitez supprimer la stratégie.

La stratégie est supprimée.

Afficher les données de trafic réseau

Vous pouvez surveiller le trafic réseau en consultant les graphiques disponibles à partir de la page règles de classification du trafic.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

- Vous disposez de l'autorisation d'accès racine ou des droits d'accès aux comptes de tenant.

Description de la tâche

Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service Load Balancer afin de déterminer si la stratégie limite le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la stratégie.

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.

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.			

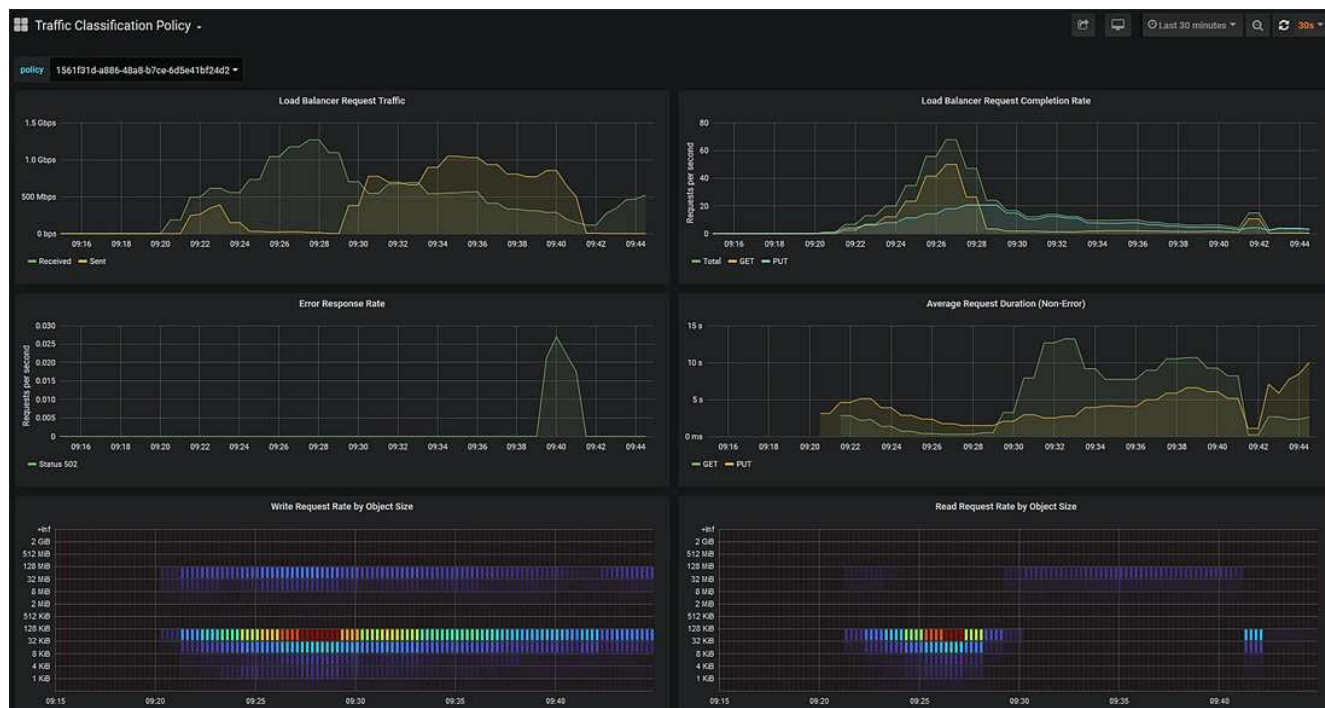


Les boutons **Create**, **Edit** et **Remove** sont désactivés si vous disposez de l'autorisation d'accès aux comptes de tenant mais que vous ne disposez pas de l'autorisation d'accès racine.

2. Sélectionnez le bouton radio à gauche de la police pour laquelle vous souhaitez afficher les mesures.
3. Sélectionnez **métriques**.

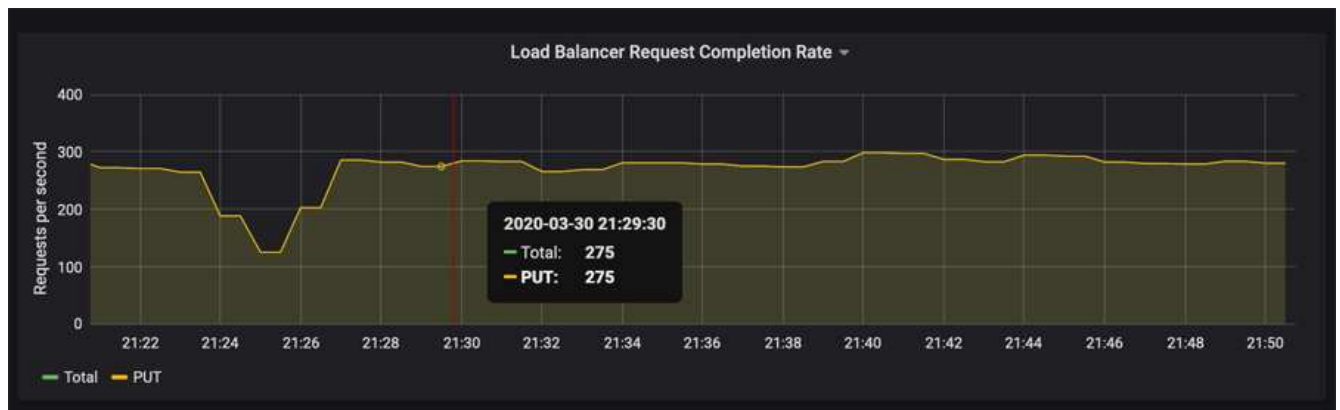
Une nouvelle fenêtre de navigateur s'ouvre et les graphiques de la politique de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

Vous pouvez sélectionner d'autres stratégies à afficher à l'aide de la liste déroulante **policy**.

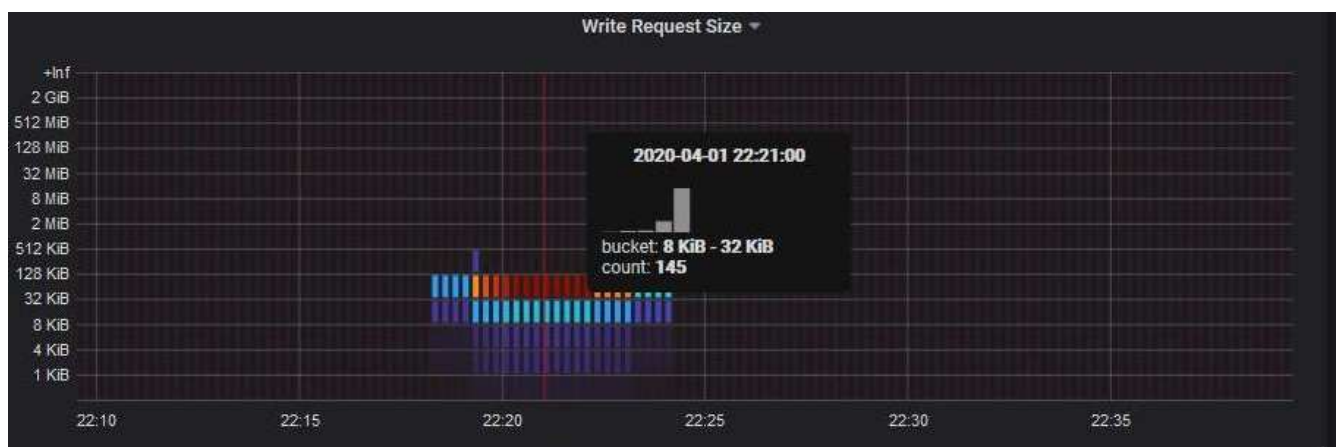


Les graphiques suivants sont inclus sur la page Web.

- Trafic des demandes d'équilibrage de charge : ce graphique fournit une moyenne mobile de 3 minutes du débit des données transmises entre les terminaux d'équilibreur de charge et les clients effectuant les demandes, en bits par seconde.
 - Taux d'exécution de la demande d'équilibrage de charge : ce graphique fournit une moyenne mobile de 3 minutes du nombre de demandes terminées par seconde, ventilées par type de demande (GET, PUT, HEAD et DELETE). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle demande ont été validés.
 - Taux de réponse d'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.
 - Durée moyenne de la demande (non-erreur) : ce graphique fournit une moyenne mobile de 3 minutes de durée de la demande, 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 demande d'écriture par taille d'objet : cette configuration fournit une moyenne mobile de 3 minutes du taux de traitement des demandes d'écriture basé sur la taille de l'objet. Dans ce contexte, les demandes d'écriture ne font référence qu'à DES requêtes PUT.
 - Taux de demande de lecture par taille d'objet : cette carte thermique fournit une moyenne mobile de 3 minutes du taux de traitement des demandes de lecture en fonction de la taille de l'objet. Dans ce contexte, les demandes de lecture ne font référence qu'à L'OBTENTION des demandes. Les couleurs de la carte de chaleur indiquent la fréquence relative d'une taille d'objet dans un graphique individuel. Les couleurs plus froides (par exemple, le violet et le bleu) indiquent des taux relatifs plus bas, et les couleurs plus chaudes (par exemple, l'orange et le rouge) indiquent des taux relatifs plus élevés.
4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.



5. Placez le curseur sur une carte de chaleur pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objet agrégées dans le compte et le nombre de demandes par seconde pendant cette période.



6. Utilisez le menu déroulant **Policy** en haut à gauche pour sélectionner une autre stratégie.

Les graphiques de la stratégie sélectionnée s'affichent.

7. Vous pouvez également accéder aux graphiques à partir du menu **SUPPORT**.
 - a. Sélectionnez **SUPPORT Outils métriques**.
 - b. Dans la section **Grafana** de la page, sélectionnez **politique de classification du trafic**.
 - c. Sélectionnez la police dans le menu déroulant situé en haut à gauche de la page.

Les politiques de classification du trafic sont identifiées par leur ID. Les ID de police sont répertoriés sur la page règles de classification de la circulation.

8. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Informations associées

[Surveiller et résoudre les problèmes](#)

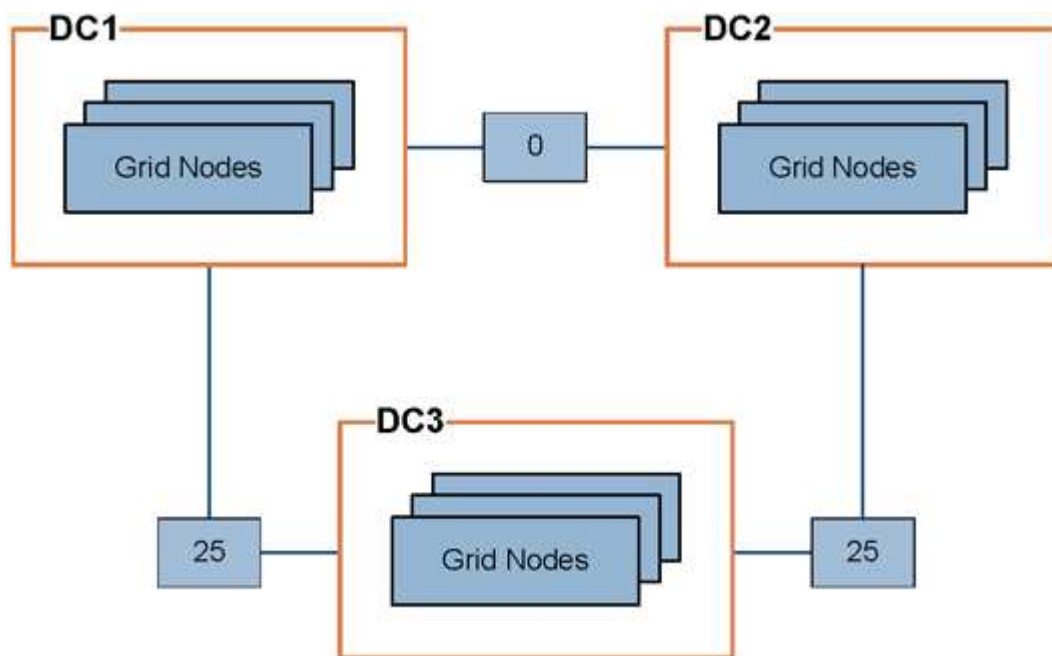
Gérer les coûts de liaison

Quels sont les coûts de liaison

Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

- Les coûts des liens permettent de classer par ordre de priorité la copie d'objet utilisée pour les récupérations d'objets.
- Les coûts des liaisons sont utilisés par l'API de gestion du grid et l'API de gestion des locataires pour déterminer quels services StorageGRID internes utiliser.
- Les coûts de liaison sont utilisés par le service CLB (Connection Load Balancer) obsolète sur les nœuds de passerelle pour diriger les connexions client. Voir [Fonctionnement de l'équilibrage de charge - service CLB](#).

Le schéma présente une grille de trois sites avec des coûts de liaison configurés entre les sites :



- Le service CLB sur les nœuds de passerelle distribue également les connexions client à tous les nœuds de stockage du même site de data Center et à tous les sites de data Center dont le coût de liaison est 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 l'exemple, si une application client de DC2 récupère un objet stocké à la fois à DC1 et DC3, l'objet est récupéré de DC1, car le coût de liaison de DC1 à DC2 est 0, ce qui est inférieur au coût de liaison de DC3 à DC2 (25).

Les coûts de liaison sont des nombres relatifs arbitraires sans unité de mesure spécifique. Par exemple, un coût de lien de 50 est utilisé de manière moins préférentielle qu'un coût de lien de 25. Le tableau 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.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation Configuration de la page de topologie de la grille.

Étapes

1. Sélectionnez **CONFIGURATION réseau coût de liaison**.

Link Cost
Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination	Actions
10	20	

2. Sélectionnez un site sous **Link Source** et entrez une valeur de coût comprise entre 0 et 100 sous **Link destination**.

Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

Pour annuler les modifications, sélectionnez **Retour**.

3. Sélectionnez **appliquer les modifications**.

Utiliser AutoSupport

Qu'est-ce que AutoSupport ?

La fonctionnalité AutoSupport permet à votre système StorageGRID d'envoyer des messages d'état et d'état au support technique.

L'utilisation de AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes. Le support technique peut également surveiller les besoins en stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. Vous pouvez également configurer l'envoi des messages AutoSupport à une destination supplémentaire.

Informations incluses dans les messages AutoSupport

Les messages AutoSupport incluent des informations telles que :

- Version du logiciel StorageGRID
- Version du système d'exploitation
- Informations sur les attributs au niveau du système et de l'emplacement
- Alertes et alarmes récentes (système hérité)
- État actuel de toutes les tâches de la grille, y compris les données historiques
- Utilisation de la base de données du nœud d'administration
- Nombre d'objets perdus ou manquants
- Paramètres de configuration de la grille
- Entités NMS
- Règle ILM active
- Fichier de spécification de grille provisionné
- Les mesures de diagnostic

Vous pouvez activer la fonctionnalité AutoSupport et les options AutoSupport individuelles lors de la première installation de StorageGRID, ou vous pouvez les activer ultérieurement. Si AutoSupport n'est pas activé, un message s'affiche dans le tableau de bord de Grid Manager. Le message inclut un lien vers la page de configuration de AutoSupport.

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



Si vous fermez le message, il n'apparaîtra plus tant que le cache de votre navigateur n'aura pas été effacé, même si AutoSupport reste désactivé.

Qu'est-ce que Digital Advisor ?

Digital Advisor est une solution cloud qui exploite l'analytique prédictive et les connaissances de la communauté issues de la base installée de NetApp. Les évaluations continues des risques, les alertes

prédictives, les conseils normatifs et les actions automatisées vous aident à anticiper les problèmes, ce qui permet d'améliorer l'état et la disponibilité du système.

Vous devez activer AutoSupport si vous souhaitez utiliser les tableaux de bord et les fonctionnalités de Digital Advisor sur le site de support NetApp.

["Documentation Digital Advisor"](#)

Protocoles pour l'envoi des messages AutoSupport

Vous pouvez choisir l'un des trois protocoles pour l'envoi des messages AutoSupport :

- HTTPS
- HTTP
- SMTP

Si vous envoyez des messages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique.

Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP.

Options AutoSupport

Toutes les combinaisons d'options suivantes vous permettent d'envoyer des messages AutoSupport au support technique :

- **Hebdomadaire**: Envoyer automatiquement des messages AutoSupport une fois par semaine. Paramètre par défaut : activé.
- **Event-déclenché** : envoie automatiquement des messages AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : activé.
- **On Demand**: Laissez le support technique demander à votre système StorageGRID d'envoyer automatiquement des messages AutoSupport, ce qui est utile lorsqu'ils travaillent activement en cas de problème (nécessite le protocole de transmission HTTPS AutoSupport). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des messages AutoSupport à tout moment.

Informations associées

["Support NetApp"](#)

Configurez AutoSupport

Vous pouvez activer la fonctionnalité AutoSupport et les options AutoSupport individuelles lors de la première installation de StorageGRID, ou vous pouvez les activer ultérieurement.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine ou d'une autre autorisation de configuration de grille.
- Si vous utilisez le protocole HTTPS ou HTTP pour l'envoi de messages AutoSupport, vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit à l'aide d'un serveur proxy (connexions entrantes non requises).

- Si vous utilisez le protocole HTTPS ou HTTP et que vous souhaitez utiliser un serveur proxy, vous avez [Configuré un serveur proxy d'administration](#).
- Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous avez configuré un serveur de messagerie SMTP. La même configuration de serveur de messagerie est utilisée pour les notifications par e-mail d'alarme (système hérité).

Spécifiez le protocole des messages AutoSupport

Vous pouvez utiliser les protocoles suivants pour l'envoi des messages AutoSupport :

- **HTTPS** : il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Le protocole HTTPS utilise le port 443. Pour activer la fonctionnalité AutoSupport On Demand, vous devez utiliser le protocole HTTPS.
- **HTTP**: Ce protocole n'est pas sécurisé, sauf s'il est utilisé dans un environnement de confiance où le serveur proxy se convertit en HTTPS lors de l'envoi de données via Internet. Le protocole HTTP utilise le port 80.
- **SMTP**: Utilisez cette option si vous souhaitez que les messages AutoSupport soient envoyés par e-mail. Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP sur la page Configuration des e-mails existants (**SUPPORT alarmes (hérité) Configuration des e-mails existants**).



SMTP était le seul protocole disponible pour les messages AutoSupport avant la version de StorageGRID 11.2. Si vous avez installé une version antérieure de StorageGRID au départ, SMTP est peut-être le protocole sélectionné.

Le protocole que vous définissez permet d'envoyer tous les types de messages AutoSupport.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.

La page AutoSupport s'affiche et l'onglet **Paramètres** est sélectionné.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Protocol Details

Protocol ?

☒ HTTPS
☐ HTTP
☐ SMTP

NetApp Support Certificate Validation ?

Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

☒

Enable Event-Triggered AutoSupport ?

☒

Enable AutoSupport on Demand ?

☐

Software Updates

Check for software updates ?

☒

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

☐

Save

Send User-Triggered AutoSupport

- Sélectionnez le protocole à utiliser pour envoyer des messages AutoSupport.
- Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat TLS pour sécuriser la connexion au serveur de support NetApp.
 - **Utiliser le certificat de support NetApp** (par défaut) : la validation du certificat permet de garantir la sécurité de la transmission des messages AutoSupport. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
 - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple lorsqu'il y a un problème temporaire avec un certificat.
- Sélectionnez **Enregistrer**.

Tous les messages hebdomadaires, déclenchés par l'utilisateur et déclenchés par des événements sont envoyés à l'aide du protocole sélectionné.

Désactiver les messages AutoSupport hebdomadaires

Par défaut, le système StorageGRID est configuré pour envoyer un message AutoSupport au support NetApp une fois par semaine.

Pour déterminer quand le message hebdomadaire AutoSupport sera envoyé, accédez à l'onglet **AutoSupport Résultats**. Dans la section **AutoSupport hebdomadaire**, examinez la valeur de **prochaine heure programmée**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time ⓘ 2021-09-14 21:10:00 MDT

Most Recent Result ⓘ Idle (NetApp Support)

Last Successful Time ⓘ N/A (NetApp Support)

Vous pouvez désactiver l'envoi automatique de messages AutoSupport hebdomadaires à tout moment.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactivez les messages AutoSupport déclenchés par les événements

Par défaut, le système StorageGRID est configuré de manière à envoyer un message AutoSupport au support NetApp lorsqu'une alerte importante ou un autre événement système important se produit.

Vous pouvez désactiver à tout moment les messages AutoSupport déclenchés par les événements.



Les messages AutoSupport déclenchés par des événements sont également supprimés lorsque vous supprimez des notifications par e-mail dans tout le système. (Sélectionnez **CONFIGURATION système Options d'affichage**. Sélectionnez ensuite **Supprimer toutes les notifications**.)

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.
2. Décochez la case **Activer AutoSupport déclenchée par événement**.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport on Demand

AutoSupport On Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

AutoSupport On Demand est désactivé par défaut. L'activation de cette fonction permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des messages AutoSupport. Le support technique peut également définir l'intervalle d'interrogation pour les requêtes AutoSupport On Demand.

Le support technique ne peut ni activer ni désactiver AutoSupport On Demand.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.
2. Sélectionnez le **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport On Demand**.
5. Sélectionnez **Enregistrer**.

AutoSupport On Demand est activé et le support technique peut envoyer des demandes AutoSupport On Demand à StorageGRID.

Désactive les vérifications des mises à jour logicielles

Par défaut, StorageGRID contacte NetApp pour déterminer si des mises à jour logicielles sont disponibles pour votre système. Si un correctif StorageGRID ou une nouvelle version est disponible, la nouvelle version s'affiche sur la page mise à niveau StorageGRID.

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'un accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.
2. Désélectionnez la case à cocher **Rechercher les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les messages d'état et d'état sont envoyés au support NetApp. Vous pouvez indiquer une destination supplémentaire pour tous les messages AutoSupport.

Pour vérifier ou modifier le protocole utilisé pour envoyer des messages AutoSupport, reportez-vous aux instructions à [Spécifiez le protocole des messages AutoSupport](#).



Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des messages AutoSupport à une destination supplémentaire.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.
2. Sélectionnez **Activer une destination AutoSupport supplémentaire**.

Les champs destination AutoSupport supplémentaire s'affichent.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination  ☒

Hostname 

Port 

Certificate Validation 

You are not using a TLS certificate to secure the connection to the additional AutoSupport destination.

Save

Send User-Triggered AutoSupport

- Entrez le nom d'hôte ou l'adresse IP du serveur d'un serveur de destination AutoSupport supplémentaire.



Vous ne pouvez entrer qu'une destination supplémentaire.

- Entrez le port utilisé pour la connexion à un serveur de destination AutoSupport supplémentaire (le port par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS).
- Pour envoyer vos messages AutoSupport avec validation de certificat, sélectionnez **utiliser le bundle de CA personnalisé** dans la liste déroulante **validation de certificat**. Puis, effectuez l'une des opérations suivantes :
 - Utilisez un outil d'édition pour copier et coller tout le contenu de chacun des fichiers de certificat d'autorité de certification codés au PEM dans le champ **CA bundle**, concaténé dans l'ordre de la chaîne de certificats. Vous devez inclure `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` dans votre sélection.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination  ☒

Hostname 

Port 

Certificate Validation 

CA Bundle 

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz123456780ABCDEFGHIJKL  
123456/7890ABCDEFGHIabcdefghijklmnopqrstuvwxyzABCD  
-----END CERTIFICATE-----
```

Browse

- Sélectionnez **Parcourir**, naviguez jusqu'au fichier contenant les certificats, puis sélectionnez **Ouvrir** pour télécharger le fichier. La validation du certificat garantit que la transmission des messages

AutoSupport est sécurisée.

6. Pour envoyer vos messages AutoSupport sans validation de certificat, sélectionnez **ne pas vérifier le certificat** dans la liste déroulante **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.

Un message d'avertissement s'affiche : « vous n'utilisez pas de certificat TLS pour sécuriser la connexion à la destination AutoSupport supplémentaire. »

7. Sélectionnez **Enregistrer**.

Tous les futurs messages AutoSupport hebdomadaires, déclenchés par les événements et déclenchés par l'utilisateur seront envoyés à la destination supplémentaire.

Déclencher manuellement un message AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement un message AutoSupport à envoyer.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine ou d'une autre autorisation de configuration de grille.

Étapes

1. Sélectionnez **SUPPORT Outils AutoSupport**.

La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

StorageGRID tente d'envoyer un message AutoSupport au support technique. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat** la plus récente est mise à jour sur "échec" et StorageGRID n'essaie pas d'envoyer à nouveau le message AutoSupport.



Après avoir envoyé un message AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport de votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Dépanner les messages AutoSupport

Si la tentative d'envoi d'un message AutoSupport échoue, le système StorageGRID effectue différentes actions en fonction du type de message AutoSupport. Vous pouvez vérifier l'état des messages AutoSupport en sélectionnant **SUPPORT Outils AutoSupport Résultats**.



Les messages AutoSupport déclenchés par des événements sont supprimés lorsque vous supprimez des notifications par e-mail dans tout le système. (Sélectionnez **CONFIGURATION système Options d'affichage**. Sélectionnez ensuite **Supprimer toutes les notifications**.)

Lorsque le message AutoSupport ne parvient pas à envoyer, ""FAILED"" s'affiche dans l'onglet **Résultats** de la page **AutoSupport**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time ? 2020-12-11 23:30:00 EST

Most Recent Result ? Idle (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

Event-Triggered AutoSupport

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

User-Triggered AutoSupport

Most Recent Result ? Failed (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

AutoSupport On Demand

AutoSupport On Demand messages are only sent to NetApp Support.

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

Échec hebdomadaire du message AutoSupport

Si un message AutoSupport hebdomadaire ne parvient pas à s'envoyer, le système StorageGRID prend les actions suivantes :

1. Met à jour l'attribut de résultat le plus récent pour réessayer.
2. Tente de renvoyer le message AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échec d'envoi, met à jour l'attribut de résultat le plus récent sur échec.
4. Tente à nouveau d'envoyer un message AutoSupport à l'heure programmée suivante.
5. Maintient le programme AutoSupport normal si le message échoue parce que le service NMS n'est pas disponible et si un message est envoyé avant sept jours.
6. Lorsque le service NMS est de nouveau disponible, envoie immédiatement un message AutoSupport si

aucun message n'a été envoyé pendant sept jours ou plus.

Échec du message AutoSupport déclenché par l'utilisateur ou déclenché par un événement

Si l'envoi d'un message AutoSupport déclenché par l'utilisateur ou un événement ne parvient pas à s'effectuer, le système StorageGRID prend les actions suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir les paramètres de configuration corrects de la messagerie, l'erreur suivante s'affiche :
`AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Ne tente pas d'envoyer le message à nouveau.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution (**SUPPORT alarmes (hérité)** * Configuration de l'e-mail héritée*). Le message d'erreur suivant peut apparaître sur la page AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Découvrez comment configurer les paramètres du serveur de messagerie dans le [instructions de contrôle et de dépannage](#).

Corrigez l'échec d'un message AutoSupport

En cas d'échec et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution. Le message d'erreur suivant peut apparaître sur la page AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyez des messages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer des messages AutoSupport E-Series SANtricity System Manager au support technique par l'intermédiaire d'un nœud d'administration StorageGRID plutôt que du port de gestion de l'appliance de stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation Administrateur de l'appliance de stockage ou de l'autorisation d'accès racine.



Vous devez disposer du firmware SANtricity 8.70 (11.7) ou version ultérieure pour accéder à SANtricity System Manager via Grid Manager.

Description de la tâche

Les messages AutoSupport E-Series contiennent des informations détaillées sur le matériel de stockage. Ils sont plus spécifiques que les autres messages AutoSupport envoyés par le système StorageGRID.

Configurez une adresse de serveur proxy spéciale dans SANtricity System Manager pour que les messages AutoSupport soient transmis par l'intermédiaire d'un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les messages AutoSupport transmis de cette façon respectent les paramètres de

proxy d'expéditeur et d'administration préférés qui peuvent avoir été configurés dans le Gestionnaire de grille.

Si vous souhaitez configurer le serveur proxy d'administration dans Grid Manager, reportez-vous à la section [Configurez les paramètres du proxy d'administration](#).

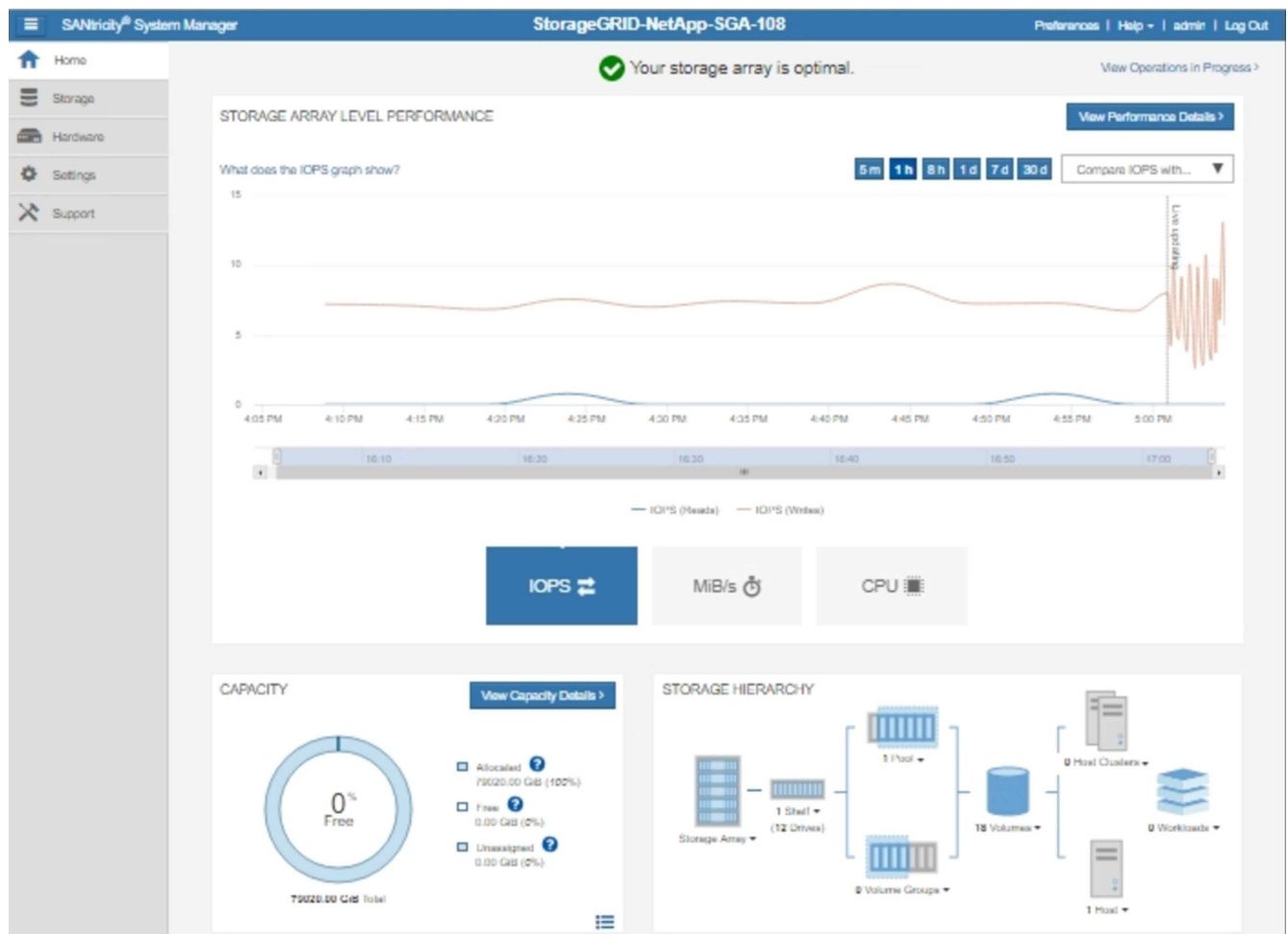


Cette procédure permet uniquement de configurer un serveur proxy StorageGRID pour les messages AutoSupport E-Series. Pour en savoir plus sur la configuration des baies E-Series AutoSupport, consultez le "[Documentation NetApp E-Series et SANtricity](#)".

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **NOEUDS**.
2. Dans la liste des nœuds de gauche, sélectionnez le nœud d'appliance de stockage à configurer.
3. Sélectionnez **SANtricity System Manager**.

La page d'accueil de SANtricity System Manager s'affiche.



4. Sélectionnez **SUPPORT support Center AutoSupport**.

La page opérations AutoSupport s'affiche.

Technical Support

Chassis serial number: 031517000693

NetApp My Support 

US/Canada 888.463.8277

Other Contacts

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

Enable/Disable AutoSupport Features

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

Configure AutoSupport Delivery Method

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

Schedule AutoSupport Dispatches

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

Send AutoSupport Dispatch

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

View AutoSupport Log

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

Enable AutoSupport Maintenance Window

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

Disable AutoSupport Maintenance Window

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Sélectionnez **configurer la méthode de livraison AutoSupport**.

La page configurer la méthode de livraison AutoSupport s'affiche.

6. Sélectionnez **HTTPS** pour la méthode de livraison.



Le certificat qui active le protocole HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.

8. Entrez `tunnel-host` Pour l'adresse **hôte**.

`tunnel-host` Est l'adresse spéciale pour utiliser un nœud d'administration pour envoyer les messages AutoSupport E-Series.

9. Entrez `10225` Pour le **Numéro de port**.

`10225` Numéro de port sur le serveur proxy StorageGRID qui reçoit des messages AutoSupport du contrôleur E-Series de l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport.

Si c'est le cas, un message apparaît dans une bannière verte : « votre configuration AutoSupport a été

vérifiée ».

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez les paramètres DNS de StorageGRID et la mise en réseau, assurez-vous que le nœud d'administration d'expéditeur privilégié peut se connecter au site du support NetApp, puis réessayez.

11. Sélectionnez **Enregistrer**.

La configuration est enregistrée et un message de confirmation apparaît : « la méthode de livraison AutoSupport a été configurée ».

Gérer des nœuds de stockage

À propos de la gestion des nœuds de stockage

Des nœuds de stockage fournissent de la capacité de stockage sur disque et des services. La gestion des nœuds de stockage implique les tâches suivantes :

- Gestion des options de stockage
- Description des filigranes du volume de stockage et utilisation des filigranes pour contrôler le moment où les nœuds de stockage deviennent en lecture seule
- Contrôle et gestion de l'espace utilisé pour les métadonnées d'objet
- Configuration des paramètres globaux des objets stockés
- Application des paramètres de configuration du nœud de stockage
- Gestion des nœuds de stockage complets

Qu'est-ce qu'un nœud de stockage ?

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Chaque système StorageGRID doit disposer d'au moins trois nœuds de stockage. Si vous avez plusieurs sites, chaque site de votre système StorageGRID doit également disposer de trois nœuds de stockage.

Un nœud de stockage inclut les services et les processus nécessaires pour stocker, déplacer, vérifier et récupérer les données d'objet et les métadonnées sur le disque. Vous pouvez afficher des informations détaillées sur les nœuds de stockage sur la page **NODES**.

Qu'est-ce que le service ADC ?

Le service contrôleur de domaine d'administration (ADC) authentifie les nœuds de la grille et leurs connexions entre eux. Le service ADC est hébergé sur chacun des trois premiers nœuds de stockage d'un site.

Le service ADC conserve les informations de topologie, notamment l'emplacement et la disponibilité des services. Lorsqu'un nœud de grille nécessite des informations provenant d'un autre nœud de grille ou qu'une action soit effectuée par un autre nœud de grille, il contacte un service ADC pour trouver le nœud de grille le plus adapté au traitement de sa demande. De plus, le service ADC conserve une copie des packs de configuration du déploiement StorageGRID, ce qui permet à n'importe quel nœud de la grille de récupérer les informations de configuration actuelles. vous pouvez afficher les informations ADC d'un nœud de stockage sur la page topologie de la grille (**PRISE EN CHARGE topologie de la grille**).

Pour faciliter les opérations distribuées et en attente, chaque service ADC synchronise les certificats, les lots

de configuration et les informations sur les services et la topologie avec les autres services ADC du système StorageGRID.

En général, tous les nœuds de la grille maintiennent une connexion à au moins un service ADC. Les nœuds du grid accèdent ainsi aux informations les plus récentes. Lorsque les nœuds de la grille se connectent, ils mettent en cache les certificats d'autres nœuds de la grille, ce qui permet aux systèmes de continuer à fonctionner avec les nœuds de la grille connus même lorsqu'un service ADC n'est pas disponible. Les nouveaux nœuds de grille ne peuvent établir de connexions qu'à l'aide d'un service ADC.

La connexion de chaque nœud de grille permet au service ADC de collecter les informations de topologie. Ces informations sur le nœud de la grille incluent la charge CPU, l'espace disque disponible (si le système dispose de stockage), les services pris en charge et l'ID de site du nœud de la grille. D'autres services demandent au service ADC d'obtenir des informations sur la topologie par le biais de requêtes de topologie. Le service ADC répond à chaque requête avec les dernières informations reçues du système StorageGRID.

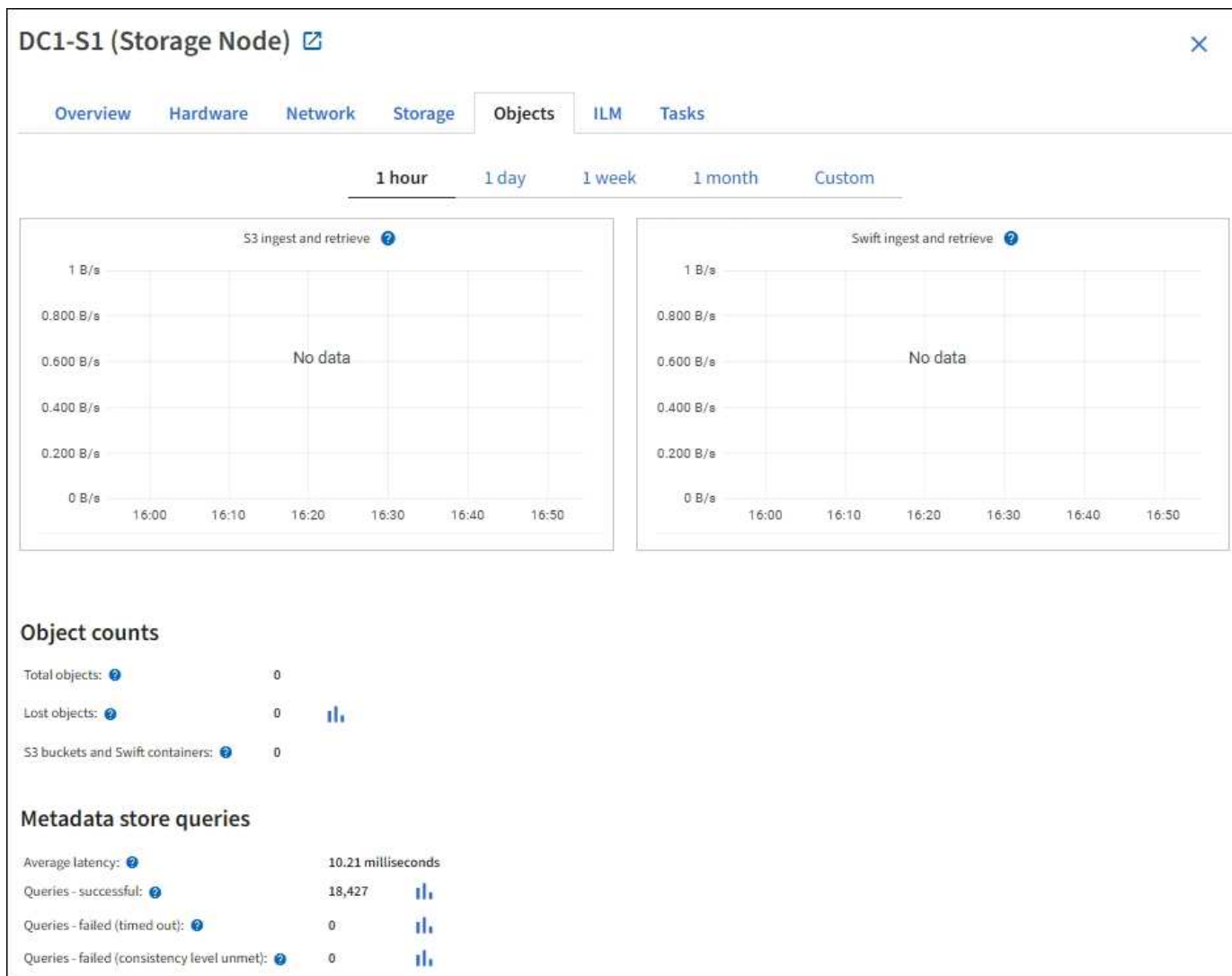
Qu'est-ce que le service DDS ?

Hébergé par un nœud de stockage, le service DDS (Distributed Data Store) s'interface avec la base de données Cassandra pour effectuer des tâches en arrière-plan sur les métadonnées d'objet stockées dans le système StorageGRID.

Nombre d'objets

Le service DDS suit le nombre total d'objets ingérés dans le système StorageGRID, ainsi que le nombre total d'objets ingérés par chacune des interfaces prises en charge par le système (S3 ou Swift).

Vous pouvez voir le nombre total d'objets dans l'onglet objets de la page noeuds pour n'importe quel noeud de stockage.



Requêtes

Vous pouvez identifier le temps moyen d'exécution d'une requête sur le magasin de métadonnées par le biais du service DDS spécifique, du nombre total de requêtes réussies et du nombre total de requêtes ayant échoué en raison d'un problème de délai d'attente.

Un examen des informations de requête peut être nécessaire afin de contrôler l'état du datastore Cassandra, ce qui a un impact sur les performances d'entrée et de récupération du système. Par exemple, si la latence d'une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d'attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d'échecs de cohérence. Les échecs de niveau de cohérence résultent d'un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est effectuée par le biais du service DDS spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille. Voir [Exécuter les diagnostics](#).

Garanties et contrôles de cohérence

StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Toute opération GET après une opération PUT réussie sera capable de lire les données récemment écrites. Les écrasements

d'objets existants, les mises à jour de métadonnées et les suppressions restent cohérents.

Qu'est-ce que le service LDR ?

Hébergé par chaque nœud de stockage, le service LDR (local distribution Router) gère le transport de contenu pour le système StorageGRID. Le transport de contenu englobe de nombreuses tâches, dont le stockage des données, le routage et le traitement des demandes. Le service LDR fait la majorité des efforts considérables du système StorageGRID en gérant les charges de transfert de données et les fonctions de trafic de données.

Le service LDR gère les tâches suivantes :

- Requêtes
- Activité liée à la gestion du cycle de vie des informations (ILM)
- Suppression d'objet
- Stockage des données objet
- Transferts de données objet à partir d'un autre service LDR (nœud de stockage)
- Gestion du stockage des données
- Interfaces de protocole (S3 et Swift)

Le service LDR gère également le mappage d'objets S3 et Swift vers des UUID (« content handle ») uniques que le système StorageGRID attribue à chaque objet ingéré.

Requêtes

Les requêtes LDR incluent des requêtes pour l'emplacement des objets lors des opérations de récupération et d'archivage. Vous pouvez identifier le temps moyen d'exécution d'une requête, le nombre total de requêtes réussies et le nombre total de requêtes ayant échoué en raison d'un problème de délai d'attente.

Vous pouvez examiner les informations de requête afin de contrôler l'état du magasin de métadonnées, ce qui a un impact sur les performances d'entrée et de récupération du système. Par exemple, si la latence d'une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d'attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d'échecs de cohérence. Les défaillances de niveau de cohérence résultent d'un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est exécutée via le service LDR spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille. Voir [Exécuter les diagnostics](#).

Activité des règles ILM

Les metrics de gestion du cycle de vie des informations vous permettent de surveiller la vitesse à laquelle les objets sont évalués pour la mise en œuvre de ILM. Vous pouvez afficher ces mesures sur le tableau de bord ou sur **NOEUDS Storage Node ILM**.

Magasins d'objets

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

Vous pouvez voir les magasins d'objets d'un nœud de stockage dans l'onglet stockage de la page nœuds.

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

Les magasins d'objets d'un nœud de stockage sont identifiés par un nombre hexadécimal compris entre 0000 et 002F, appelé ID de volume. L'espace est réservé dans le premier magasin d'objets (volume 0) pour les métadonnées d'objet dans une base de données Cassandra. Tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres magasins d'objets sont exclusivement utilisés pour les données d'objet, notamment les copies répliquées et les fragments avec code d'effacement.

Pour garantir même l'utilisation de l'espace pour les copies répliquées, les données d'objet d'un objet donné sont stockées dans un magasin d'objets basé sur l'espace de stockage disponible. Lorsqu'un ou plusieurs magasins d'objets sont remplis à la capacité, les magasins d'objets restants continuent de stocker des objets jusqu'à ce qu'il n'y ait plus d'espace sur le nœud de stockage.

Protection des métadonnées

Les métadonnées de l'objet sont des informations liées ou une description d'un objet. Par exemple, l'heure de modification de l'objet ou l'emplacement de stockage. StorageGRID stocke les métadonnées d'objet dans une base de données Cassandra, qui assure l'interface avec le service LDR.

Pour assurer la redondance et ainsi la protection contre la perte, trois copies des métadonnées d'objet sont conservées sur chaque site. Les copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site. Cette réplication n'est pas configurable et se fait automatiquement.

[Gérer le stockage des métadonnées d'objet](#)

Gérer les options de stockage

Les options de stockage incluent les paramètres de segmentation des objets, les valeurs actuelles pour les filigranes du volume de stockage et le paramètre Metadata Reserved Space. Vous pouvez également afficher les ports S3 et Swift utilisés par le service CLB obsolète sur les nœuds de passerelle et par le service LDR sur les nœuds de stockage.

Pour plus d'informations sur les affectations de ports, reportez-vous à la section [Résumé : adresses IP et ports pour les connexions client](#).

Storage Options

Overview

Configuration



Storage Options Overview

Updated: 2021-11-23 11:01:41 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

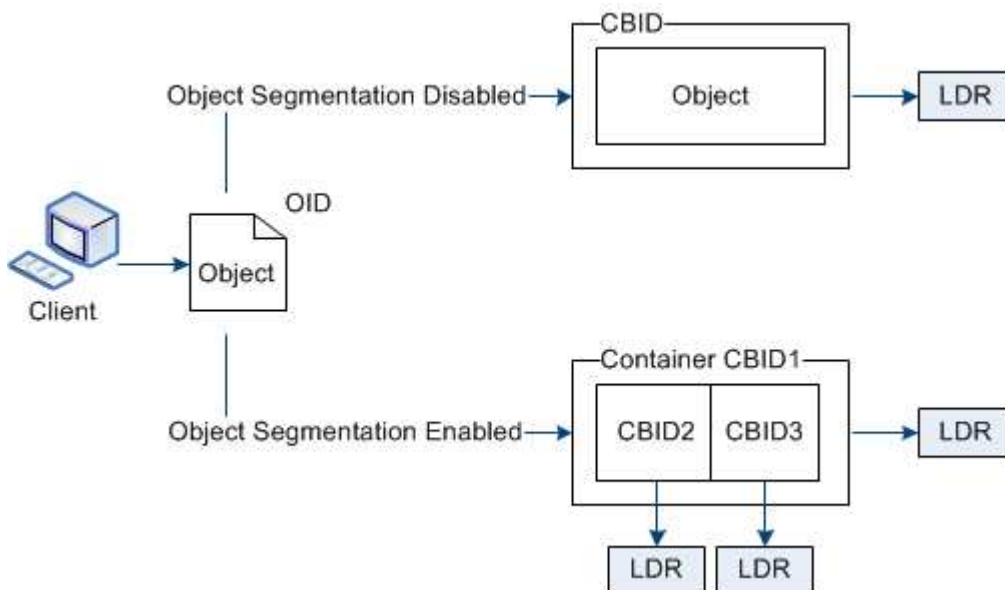
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Qu'est-ce que la segmentation d'objet ?

La segmentation d'objet consiste à diviser un objet en un ensemble d'objets de plus petite taille afin d'optimiser l'utilisation des ressources et du stockage pour les objets volumineux. 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 :

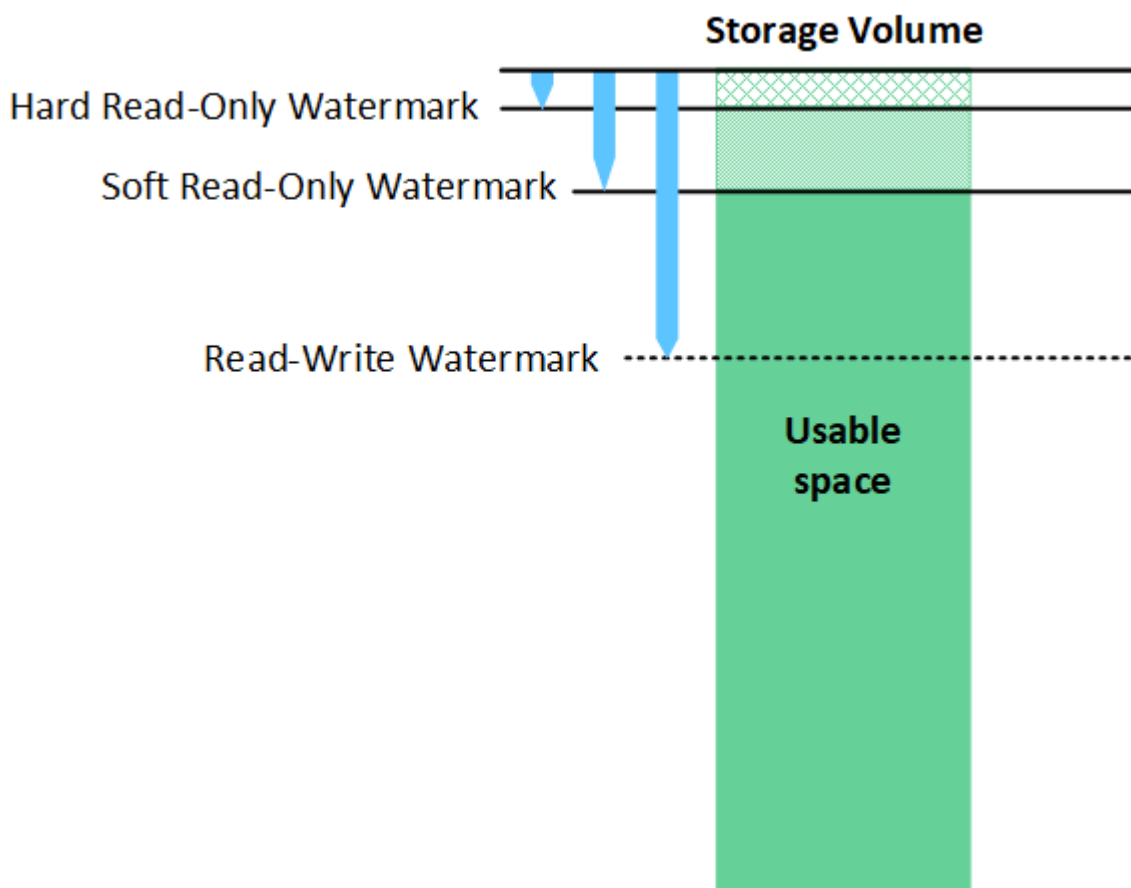
conteneur de segments + segment 1 + segment 2 = trois objets stockés

Vous pouvez améliorer les performances lors de la manipulation d'objets volumineux en vous assurant que :

- Chaque passerelle et nœud de stockage dispose d'une bande passante réseau suffisante pour le débit requis. Par exemple, configurez des réseaux Grid et client distincts sur des interfaces Ethernet 10 Gbits/s.
- Suffisamment de nœuds de passerelle et de stockage sont déployés pour le débit requis.
- Chaque nœud de stockage dispose de performances d'E/S de disque suffisantes pour le débit requis.

Quelles sont les filigranes du volume de stockage ?

StorageGRID utilise trois filigranes de volume de stockage qui garantissent que les nœuds de stockage sont transférés en toute sécurité vers un état en lecture seule avant de s'exécuter avec un espace critique et que les nœuds de stockage ayant été transférés vers un état en lecture seule afin de devenir à nouveau en lecture/écriture.





Les filigranes du volume de stockage ne s'appliquent qu'à l'espace utilisé pour les données d'objets répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées d'objet sur le volume 0, accédez à [Gérer le stockage des métadonnées d'objet](#).

Qu'est-ce que le filigrane en lecture seule souple ?

Le filigrane **Volume de stockage en lecture seule** est le premier filigrane indiquant que l'espace utilisable d'un nœud de stockage pour les données d'objet est saturé.

Si chaque volume d'un nœud de stockage a moins d'espace libre que le filigrane en lecture seule programmable de ce volume, le nœud de stockage passe en mode *lecture seule*. Le mode lecture seule signifie que le nœud de stockage annonce des services en lecture seule au reste du système StorageGRID, mais remplit toutes les demandes d'écriture en attente.

Supposons par exemple que chaque volume d'un nœud de stockage dispose d'un filigrane en lecture seule de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode veille souple en lecture seule.

Qu'est-ce que le filigrane en lecture seule difficile ?

Le filigrane **Volume de stockage en lecture seule matérielle** est le filigrane suivant pour indiquer que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein.

Si l'espace libre d'un volume est inférieur au filigrane en lecture seule de ce volume, les écritures sur le volume échoueront. Cependant, les écritures sur d'autres volumes peuvent continuer jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leurs filigranes en lecture seule.

Supposons par exemple que chaque volume d'un nœud de stockage dispose d'un filigrane en lecture seule de 5 Go. Dès que chaque volume dispose de moins de 5 Go d'espace libre, le nœud de stockage n'accepte plus de demandes d'écriture.

Le filigrane en lecture seule est toujours inférieur au filigrane en lecture seule.

Qu'est-ce que le filigrane Read-Write ?

Le filigrane **Storage Volume Read-Write** ne s'applique qu'aux nœuds de stockage ayant été passés en mode lecture seule. Il détermine quand le nœud peut redevenir lecture-écriture. Lorsque l'espace libre sur un volume de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud revient automatiquement à l'état de lecture-écriture.

Supposons par exemple que le nœud de stockage est passé en mode lecture seule. Supposons également que chaque volume dispose d'un filigrane Read-Write de 30 Go. Dès que l'espace libre d'un volume augmente jusqu'à 30 Go, le nœud redevient read-write.

Le filigrane lu-Write est toujours plus grand que le filigrane en lecture seule et le filigrane en lecture seule.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres actuels du filigrane ainsi que les valeurs optimisées par le système. Si des filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez régler les paramètres.

Ce dont vous avez besoin

- Vous avez terminé la mise à niveau vers StorageGRID 11.6.

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.

Afficher les paramètres actuels du filigrane

Vous pouvez afficher les paramètres actuels du filigrane de stockage dans Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION système Options de stockage**.
2. Dans la section Storage Watermarks (filigranes de stockage), vérifiez les paramètres des trois remplacements de filigrane de volume de stockage.

Storage Options

Overview

Configuration



Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

- Si les remplacements de filigrane sont **0**, les trois filigranes sont optimisés pour chaque volume de stockage sur chaque nœud de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

Il s'agit du paramètre par défaut et recommandé. Vous ne devez pas mettre à jour ces valeurs. Si nécessaire, vous pouvez choisir [Afficher des filigranes de stockage optimisés](#).

- Si les remplacements de filigrane ne sont pas des valeurs 0, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Suivez les instructions pour [Dépannage des alertes de remplacement du filigrane en lecture seule faible](#) pour déterminer si vous pouvez ou devez régler les paramètres.

Afficher des filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane **Volume de stockage en lecture seule**. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

1. Sélectionnez **SUPPORT Outils métriques**.
2. Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
3. Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane **Volume de stockage en lecture seule**, l'alerte **dépassement de filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

Gérer le stockage des métadonnées d'objet

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets qui peuvent être stockés sur le système en question. Pour s'assurer que votre système StorageGRID dispose d'un espace suffisant pour stocker les nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées d'objet.

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

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

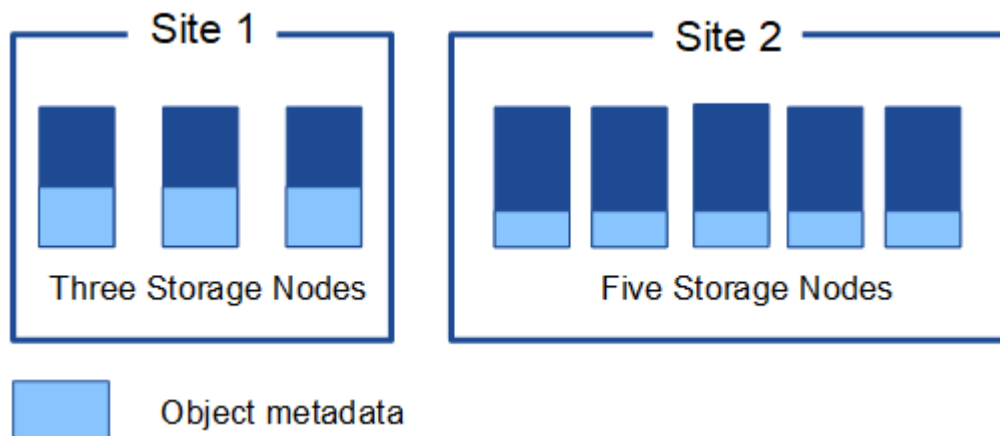
Pour un objet dans StorageGRID, les métadonnées d'objet incluent les types d'information suivants :

- Les métadonnées du système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3 ou du conteneur Swift, le nom ou l'ID du compte du locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, et la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets à plusieurs parties, les identificateurs de segment et la taille des données.

Comment les métadonnées d'objet sont-elles stockées ?

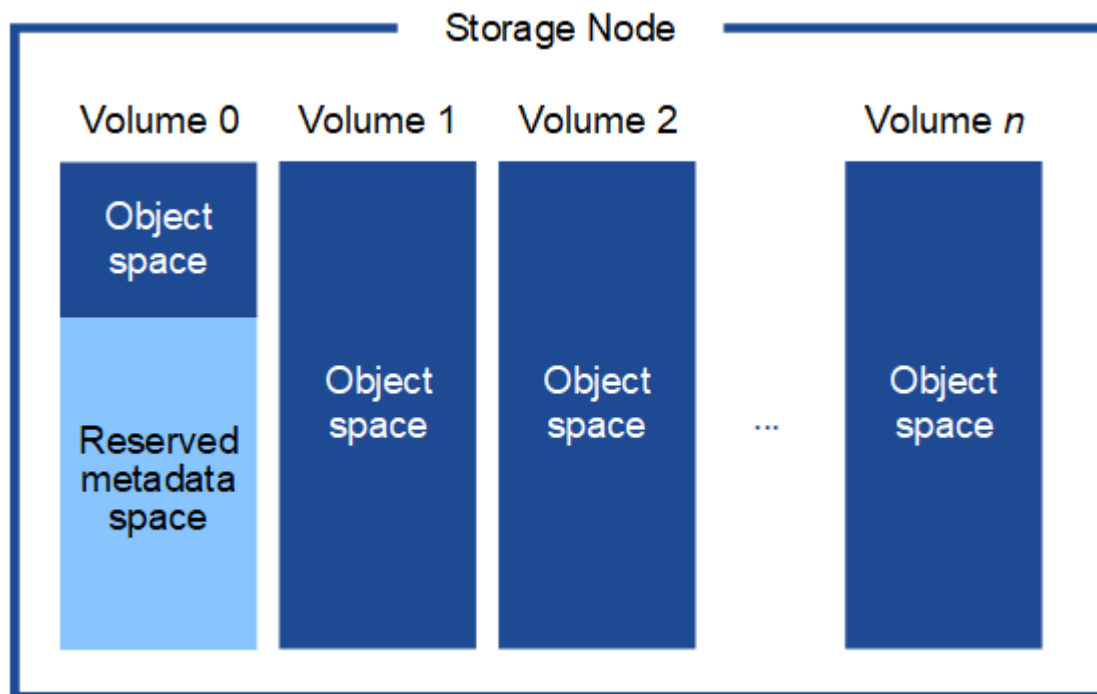
Les métadonnées d'objet sont conservées dans une base de données Cassandra, stockée indépendamment des données d'objet. StorageGRID Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque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

Cette figure représente les nœuds de stockage sur deux sites. Chaque site dispose de la même quantité de métadonnées d'objet, qui sont réparties de la même manière sur les 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 réservé aux métadonnées d'objet sur un nœud de stockage particulier dépend d'un certain nombre de facteurs, décrits ci-dessous.

Paramètre Metadata Reserved Space

Le paramètre *Metadata Reserved Space* est un paramètre à l'échelle du système qui représente la quantité d'espace qui sera réservée aux métadonnées sur le volume 0 de chaque nœud de stockage. Comme indiqué dans le tableau, la valeur par défaut de ce paramètre pour StorageGRID 11.6 est basée sur les éléments suivants :

- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- Quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut pour StorageGRID 11.6
11.5/11.6	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)

Pour afficher le paramètre espace réservé aux métadonnées de votre système StorageGRID :

1. Sélectionnez **CONFIGURATION système Options de stockage**.
2. Dans le tableau des filigranes de stockage, localisez **espace réservé de métadonnées**.



Storage Options Overview

Updated: 2021-12-10 13:53:01 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	8,000 GB

Dans la capture d'écran, la valeur **Metadata Reserved Space** est de 8,000 Go (8 To). Il s'agit du paramètre par défaut pour une nouvelle installation StorageGRID 11.6 dans laquelle chaque nœud de stockage dispose d'au moins 128 Go de RAM.

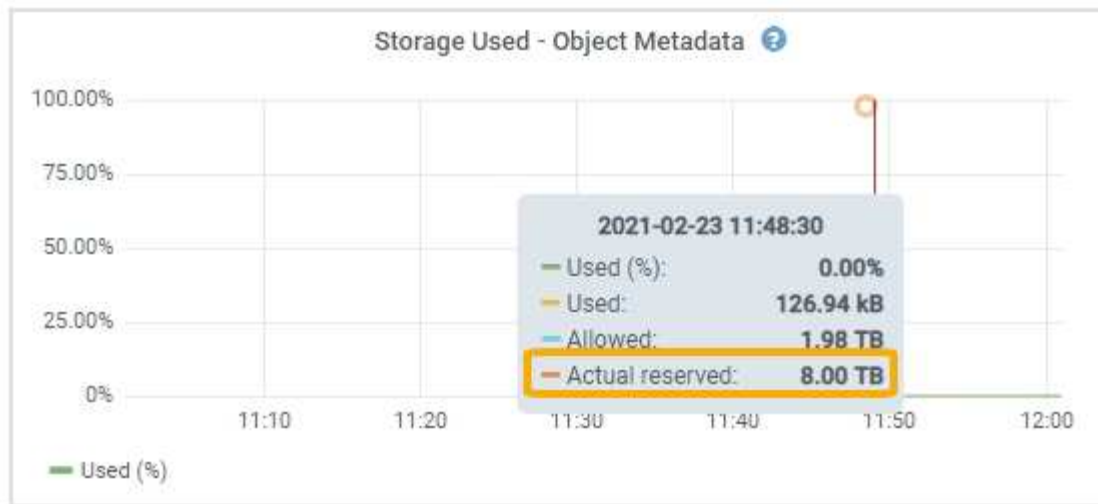
Espace réservé réel pour les métadonnées

Contrairement au paramètre espace réservé aux métadonnées pour l'ensemble du système, le paramètre *espace réservé réel* pour les métadonnées d'objet est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre espace réservé * métadonnées * pour l'ensemble du système.

Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (non utilisé en production)	10 % du volume 0
500 Go ou plus	Plus ces valeurs sont faibles : • Volume 0 • Paramètre Metadata Reserved Space

Pour afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier :

1. Dans Grid Manager, sélectionnez **NOEUDS Storage Node**.
2. Sélectionnez l'onglet **stockage**.
3. Placez le curseur sur le diagramme stockage utilisé — métadonnées objet et localisez la valeur **réservé réelle**.



Dans la capture d'écran, la valeur **réelle réservée** est de 8 To. Cette capture d'écran concerne un nœud de stockage grand format dans une nouvelle installation de StorageGRID 11.6. Étant donné que le paramètre espace réservé aux métadonnées pour l'ensemble du système est inférieur au volume 0 pour ce nœud de stockage, l'espace réservé réel pour ce nœud est égal au paramètre espace réservé aux métadonnées.

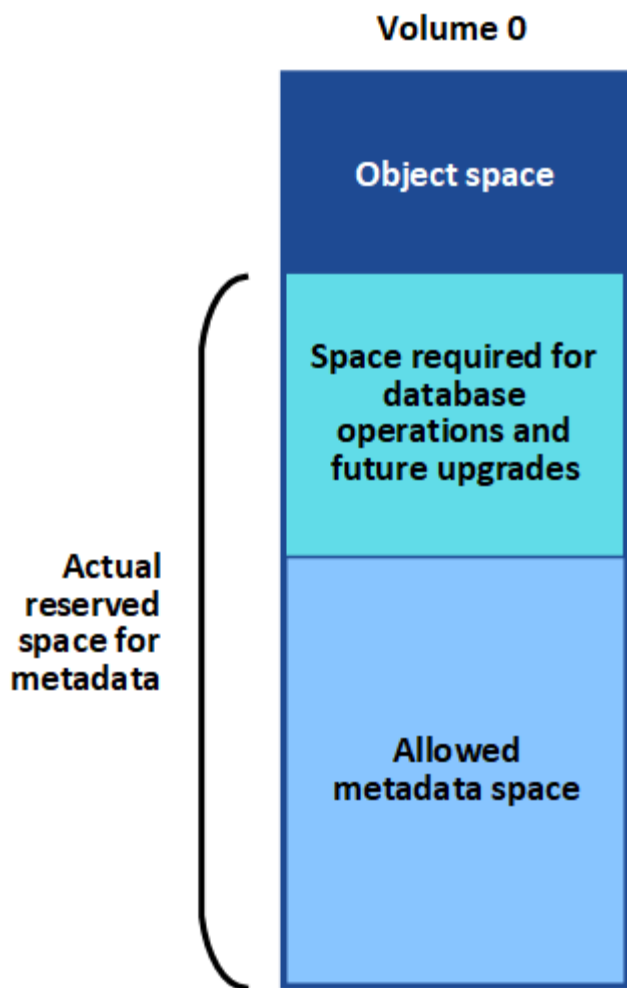
Exemple d'espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID à l'aide de la version 11.6. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.6 si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)

Espace de métadonnées autorisé

L'espace réservé réel de chaque nœud de stockage pour les métadonnées est divisé en l'espace disponible pour les métadonnées d'objet (l'espace *autorisé metadata space*) et l'espace requis pour les opérations essentielles de bases de données (telles que la compaction et la réparation) et les mises à niveau matérielles et logicielles futures. L'espace de métadonnées autorisé régit la capacité globale des objets.



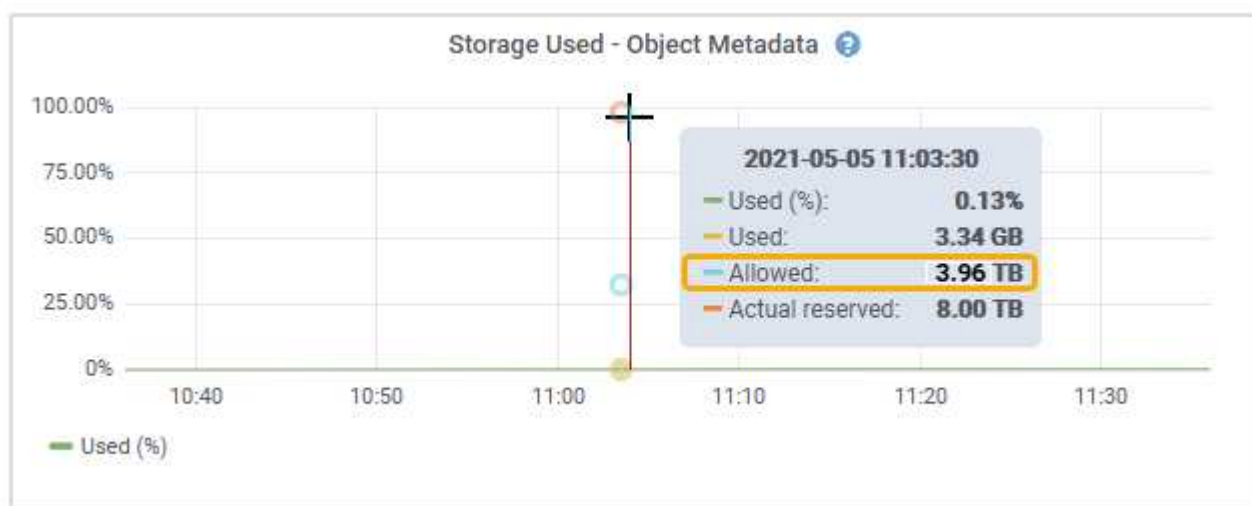
Le tableau suivant montre comment StorageGRID calcule l' **espace de métadonnées autorisé** pour différents nœuds de stockage, en fonction de la quantité de mémoire du nœud et de l'espace réservé réel pour les métadonnées.

		Quantité de mémoire sur le nœud de stockage	
	lt; 128 GB	gt;= 128 GB	Espace réservé réel pour les métadonnées
lt;= 4 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.32 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.98 To	gt; 4 TB

Pour afficher l'espace de métadonnées autorisé pour un nœud de stockage :

1. Dans Grid Manager, sélectionnez **NODES**.
2. Sélectionnez le nœud de stockage.

- Sélectionnez l'onglet **stockage**.
- Placez le curseur sur le diagramme stockage utilisé — métadonnées objet et localisez la valeur **autorisé**.



Dans la capture d'écran, la valeur **autorisé** est de 3.96 To, ce qui est la valeur maximale pour un nœud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **autorisé** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installez un système StorageGRID avec la version 11.6. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.6 lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, d'après le calcul présenté dans la [tableau pour l'espace autorisé pour les métadonnées](#): (Espace réservé réel pour les métadonnées – 1 To) × 60 %, jusqu'à un maximum de 3.96 To.

La façon dont les nœuds de stockage de différentes tailles affectent la capacité des objets

Comme décrit ci-dessus, StorageGRID distribue uniformément les métadonnées d'objet sur les nœuds de stockage sur chaque site. Par conséquent, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité des métadonnées du site.

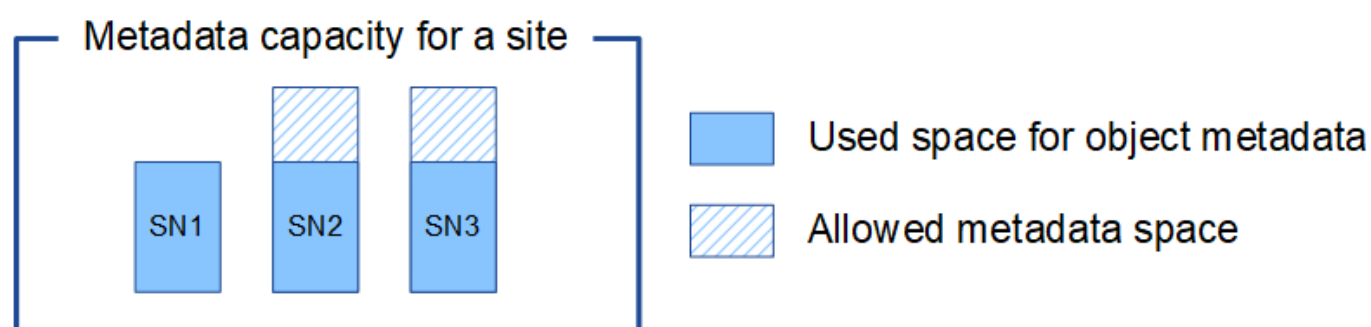
Prenons l'exemple suivant :

- Une grille sur un seul site contient trois nœuds de stockage de tailles différentes.
- Le paramètre **Metadata Reserved Space** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace réservé réel des métadonnées et l'espace

autorisé pour les métadonnées.

Nœud de stockage	Taille du volume 0	Espace réservé réel des métadonnées	Espace de métadonnées autorisé
SN1	2.2 TO	2.2 TO	1.32 TO
SN2	5 TO	4 TO	1.98 TO
SN3	6 To	4 TO	1.98 TO

Les métadonnées de l'objet sont réparties de manière uniforme sur les nœuds de stockage d'un site. En effet, chaque nœud de cet exemple ne peut contenir que 1.32 To de métadonnées. Les 0.66 To supplémentaires d'espace de métadonnées autorisé pour SN2 et SN3 ne peuvent pas être utilisés.



De même, puisque StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale des métadonnées d'un système StorageGRID est déterminée par la capacité des métadonnées d'objet du plus petit site.

Étant donné que la capacité des métadonnées contrôle le nombre maximal d'objets, lorsqu'un nœud vient à manquer de capacité de métadonnées, la grille est véritablement pleine.

Informations associées

- Pour apprendre à contrôler la capacité des métadonnées d'objet pour chaque nœud de stockage, accédez à [Surveiller et résoudre les problèmes](#).
- Pour augmenter la capacité des métadonnées d'objet de votre système, ajoutez de nouveaux nœuds de stockage. Accédez à [Développez votre grille](#).

Configurer les paramètres globaux des objets stockés

Configurer la compression des objets stockés

Vous pouvez utiliser l'option de grille Compress objets stockés pour réduire la taille des objets stockés dans StorageGRID, de sorte que les objets consomment moins de stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, l'option de grille de compression des objets stockés est désactivée. Si vous activez cette option, StorageGRID tente de compresser chaque objet lors de son enregistrement, en utilisant 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 cette option, tenez compte des points suivants :

- Vous ne devez pas activer la compression, 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, l'activation de la compression des objets stockés ne réduira pas davantage la taille d'un objet.
- N'activez pas la compression si vous utilisez NetApp FabricPool avec StorageGRID.
- Si l'option de grille objets stockés de compression est activée, les applications client S3 et Swift doivent éviter d'exécuter des opérations GET Object qui indiquent une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est inefficace de lire une plage de 10 Mo sur un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.



Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options des objets stockés, cochez la case **Compresser objets enregistrés**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Sélectionnez **Enregistrer**.

Configurez le chiffrement des objets stockés

Vous pouvez crypter les objets stockés si vous souhaitez vous assurer que les données ne peuvent pas être récupérées sous une forme lisible si un magasin d'objets est

compromis. Par défaut, les objets ne sont pas chiffrés.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Le chiffrement d'objets stocké permet le chiffrement de toutes les données d'objet à leur entrée via S3 ou Swift. 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 chiffrés restent chiffrés, mais les objets récemment ingérées ne sont pas chiffrés.



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.

Les objets stockés peuvent être cryptés à l'aide de l'algorithme de cryptage AES-128 ou AES-256.

Le paramètre de chiffrement d'objet stocké s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options d'objet stocké, définissez le chiffrement d'objet stocké sur **None** (par défaut), **AES-128** ou **AES-256**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Sélectionnez **Enregistrer**.

Configurez le hachage de l'objet stocké

L'option de hachage d'objet stocké spécifie l'algorithme de hachage utilisé pour vérifier l'intégrité des objets.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, les données d'objet sont hachées à l'aide de l'algorithme SHA-1. L'algorithme SHA-256 nécessite des ressources CPU supplémentaires et n'est généralement pas recommandé pour la vérification de l'intégrité.



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.

Étapes

1. Sélectionnez **CONFIGURATION système Options de grille**.
2. Dans la section Options des objets stockés, définissez hachage de l'objet stocké sur **SHA-1** (par défaut) ou **SHA-256**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Sélectionnez **Enregistrer**.

Paramètres de configuration du nœud de stockage

Chaque nœud de stockage utilise un certain nombre de paramètres de configuration et de compteurs. Vous devrez peut-être afficher les paramètres actuels ou réinitialiser les compteurs pour effacer les alarmes (système hérité).



Sauf en cas d'instruction spécifique dans la documentation, consultez le support technique avant de modifier les paramètres de configuration des nœuds de stockage. Si nécessaire, vous pouvez réinitialiser les compteurs d'événements pour effacer les alarmes héritées.

Pour accéder aux paramètres de configuration et aux compteurs d'un nœud de stockage :

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **site nœud de stockage**.
3. Développez le nœud de stockage et sélectionnez le service ou le composant.
4. Sélectionnez l'onglet **Configuration**.

Les tableaux suivants résument les paramètres de configuration du nœud de stockage.

LDR

Nom d'attribut	Code	Description
État HTTP	HSTE	État actuel du protocole HTTP pour S3, Swift et autre trafic StorageGRID interne : • Hors ligne : aucune opération n'est autorisée et toute application client qui tente d'ouvrir une session HTTP au service LDR reçoit un message d'erreur. Les sessions actives sont normalement fermées. • En ligne : le fonctionnement se poursuit normalement
Démarrage automatique HTTP	HTA	• Si cette option est sélectionnée, l'état du système au redémarrage dépend de l'état du composant LDR Storage. Si le composant LDR Storage est en lecture seule au redémarrage, l'interface HTTP est également en lecture seule. Si le composant LDR Storage est en ligne, alors HTTP est également en ligne. Dans le cas contraire, l'interface HTTP reste à l'état hors ligne. • Si elle n'est pas sélectionnée, l'interface HTTP reste hors ligne jusqu'à ce qu'elle soit explicitement activée.

Datastore LDR

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets perdus	RCOR	Réinitialisez le compteur du nombre d'objets perdus sur ce service.

Stockage LDR

Nom d'attribut	Code	Description
État de stockage — souhaité	SSD	Paramètre configurable par l'utilisateur pour l'état souhaité du composant de stockage. Le service LDR lit cette valeur et tente de faire correspondre l'état indiqué par cet attribut. La valeur est persistante entre les redémarrages. Par exemple, vous pouvez utiliser ce paramètre pour forcer le stockage à devenir en lecture seule, même en présence d'un espace de stockage disponible suffisant. Ceci peut être utile pour le dépannage. L'attribut peut prendre l'une des valeurs suivantes : • Hors ligne : lorsque l'état souhaité est hors ligne, le service LDR met le composant LDR Storage hors ligne. • Lecture seule : lorsque l'état souhaité est en lecture seule, le service LDR déplace l'état du stockage en lecture seule et arrête d'accepter le nouveau contenu. Notez que le contenu peut continuer à être enregistré sur le nœud de stockage pendant une courte période jusqu'à la fermeture des sessions ouvertes. • En ligne : conservez la valeur sur Online pendant le fonctionnement normal du système. L'état de stockage — le courant du composant de stockage sera défini de manière dynamique par le service en fonction de l'état du service LDR, comme le volume de l'espace de stockage objet disponible. Si l'espace est faible, le composant devient lecture seule.
Délai de vérification de l'état dépassé	SHCT	La limite de temps en secondes pendant laquelle un test de vérification de l'état doit s'effectuer pour que le volume de stockage soit considéré comme sain. Ne modifiez cette valeur que si vous y êtes invité par le support.

Vérification LDR

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets manquants	VCMI	Réinitialise le nombre d'objets manquants détectés (OMIS). Utiliser uniquement une fois la vérification de l'existence d'objet terminée. Les données d'objet répliqué manquantes sont restaurées automatiquement par le système StorageGRID.

Nom d'attribut	Code	Description
Taux de vérification	VPRI	Définissez la vitesse à laquelle la vérification des antécédents a lieu. Voir les informations sur la configuration du taux de vérification des antécédents.
Réinitialiser le nombre d'objets corrompus	VCCR	Réinitialisez le compteur pour les données d'objet répliqué corrompues trouvées lors de la vérification en arrière-plan. Cette option peut être utilisée pour effacer la condition d'alarme des objets corrompus détectés (OCOR). Pour plus d'informations, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.
Supprimer des objets en quarantaine	OQRT	Supprimez des objets corrompus du répertoire de quarantaine, réinitialisez le nombre d'objets mis en quarantaine et effacez l'alarme OQRT (Quarantaine Objects détectés). Cette option est utilisée après la restauration automatique par le système StorageGRID d'objets corrompus. Si une alarme objets perdus est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine. Dans certains cas, les objets mis en quarantaine peuvent être utiles pour la récupération des données ou pour le débogage des problèmes sous-jacents à l'origine des copies d'objet corrompues.

Codage d'effacement LDR

Nom d'attribut	Code	Description
Réinitialiser le nombre d'échecs d'écriture	RSWF	Réinitialisez le compteur pour les échecs d'écriture des données d'objet avec code d'effacement sur le nœud de stockage.
Réinitialiser le nombre d'échecs de lecture	RSRF	Réinitialisez le compteur pour les échecs de lecture des données d'objet avec code d'effacement à partir du nœud de stockage.
Réinitialiser supprime le nombre d'échecs	RSDF	Réinitialisez le compteur pour les échecs de suppression des données d'objet avec code d'effacement du nœud de stockage.
Réinitialiser le nombre de copies corrompues détectées	RSCC	Réinitialisez le compteur du nombre de copies corrompues de données d'objet avec code d'effacement sur le nœud de stockage.

Nom d'attribut	Code	Description
Réinitialiser le nombre de fragments corrompus détectés	RSCD	Réinitialisez le compteur en cas de fragments endommagés de données d'objet avec code d'effacement sur le nœud de stockage.
Réinitialiser le nombre de fragments manquants détectés	RSMD	Réinitialisez le compteur en cas de fragments manquants de données d'objet avec code d'effacement sur le nœud de stockage. Utiliser uniquement une fois la vérification de l'existence d'objet terminée.

Réplication LDR

Nom d'attribut	Code	Description
Réinitialiser le nombre d'échecs de réplication entrante	RICR	Réinitialisez le compteur pour les échecs de réplication entrants. Il peut être utilisé pour effacer l'alarme RIRF (réplication entrante — échouée).
Réinitialiser le nombre d'échecs de réplication sortante	ROCR	Réinitialisez le compteur pour les échecs de réplication sortants. Cette fonction permet d'effacer l'alarme RORF (réplifications sortantes — en échec).
Désactiver la réplication entrante	DSIR	Sélectionnez cette option pour désactiver la réplication entrante dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication entrante est désactivée, les objets peuvent être récupérés depuis le nœud de stockage pour être copiés vers d'autres emplacements du système StorageGRID, mais les objets ne peuvent pas être copiés vers ce nœud de stockage à partir d'autres emplacements : le service LDR est en lecture seule.
Désactiver la réplication sortante	DSOR	Sélectionnez cette option pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication sortante est désactivée, les objets peuvent être copiés vers ce nœud de stockage, mais les objets ne peuvent pas être récupérés depuis le nœud de stockage pour être copiés vers d'autres emplacements du système StorageGRID. Le service LDR est en écriture seule.

Informations associées

Gérer des nœuds de stockage complets

Lorsque les nœuds de stockage atteignent leur capacité maximale, ils doivent étendre le système StorageGRID en ajoutant du nouveau stockage. Trois options sont disponibles : ajout de volumes de stockage, ajout de tiroirs d'extension de stockage et ajout de nœuds de stockage.

Ajout de volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plate-forme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximum, vous pouvez ajouter des volumes pour augmenter sa capacité. Reportez-vous aux instructions pour [Extension d'un système StorageGRID](#).

Ajout de tiroirs d'extension de stockage

Certains nœuds de stockage StorageGRID, comme le SG6060, peuvent prendre en charge des tiroirs de stockage supplémentaires. Si vos appliances StorageGRID bénéficient de fonctionnalités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des tiroirs de stockage pour augmenter la capacité. Reportez-vous aux instructions pour [Extension d'un système StorageGRID](#).

Ajouter des nœuds de stockage

L'ajout de nœuds de stockage permet d'augmenter la capacité de stockage. L'ajout de stockage nécessite de prendre en compte les règles ILM et les exigences de capacité actuellement actives. Reportez-vous aux instructions pour [Extension d'un système StorageGRID](#).

Gérer les nœuds d'administration

Qu'est-ce qu'un nœud d'administration

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Chaque grid doit être connecté à un nœud d'administration principal et doit comporter un nombre quelconque de nœuds d'administration non primaires pour assurer la redondance.

Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un 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, les procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

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

Les nœuds d'administration hébergent les services suivants :

- Service AMS
- Service CMN
- Service NMS

- Service Prometheus
- Services d'équilibrage de la charge et haute disponibilité (pour prendre en charge le trafic des clients S3 et Swift)

Les nœuds d'administration prennent également en charge l'API de gestion (Management application Program interface) pour traiter les requêtes depuis l'API de gestion du grid et l'API de gestion des locataires. Voir [Utilisez l'API de gestion du grid](#).

Qu'est-ce que le service AMS

Le service du système de gestion de la vérification (AMS) suit l'activité et les événements du système.

Qu'est-ce que le service CMN

Le service de nœud de gestion de la configuration (CMN) gère les configurations de connectivité et de protocoles à l'échelle du système nécessaires à tous les services. De plus, le service CMN est utilisé pour exécuter et surveiller les tâches de la grille. Il n'y a qu'un seul service CMN par déploiement StorageGRID. Le nœud d'administration qui héberge le service CMN est appelé nœud d'administration principal.

En quoi consiste le service NMS

Le service Network Management System (NMS) alimente les options de surveillance, de rapport et de configuration affichées via le gestionnaire de grille, l'interface navigateur du système StorageGRID.

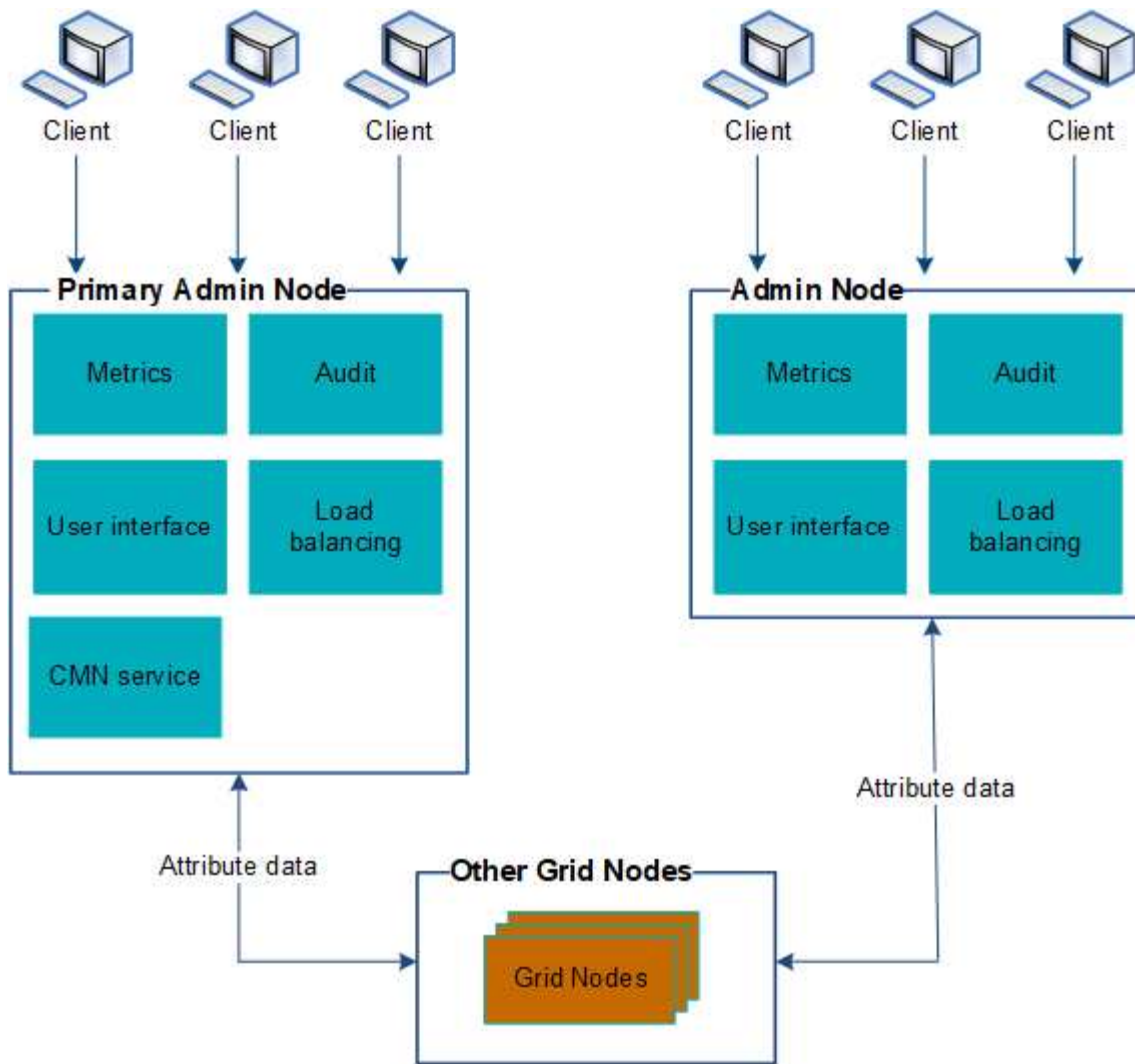
Définition du service Prometheus

Le service Prometheus collecte les metrics de séries chronologiques des services sur tous les nœuds.

Utiliser plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en cas de panne d'un nœud d'administration.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes et les alarmes (système hérité) sont toujours déclenchées et les notifications par e-mail et les messages AutoSupport sont toujours envoyés. Toutefois, plusieurs nœuds d'administration n'assurent pas la protection du basculement, à l'exception des notifications et des messages AutoSupport. En particulier, les accusés de réception d'alarme d'un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration.



Deux options s'offrent à vous pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir [Gérez les groupes haute disponibilité](#).



Lors de l'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de défaillance du nœud d'administration principal. 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

Le nœud d'administration principal héberge le service CMN. Certaines procédures de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration

principal.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **site nœud d'administration**, puis sélectionnez **+** Pour développer l'arborescence de la topologie et afficher les services hébergés sur ce nœud d'administration.

Le nœud d'administration principal héberge le service CMN.

3. Si ce nœud d'administration n'héberge pas le service CMN, vérifiez les autres nœuds d'administration.

Sélectionnez un expéditeur préféré

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, vous pouvez sélectionner le nœud d'administration qui doit être l'expéditeur préféré des notifications. Par défaut, le nœud d'administration principal est sélectionné, mais n'importe quel nœud d'administration peut être l'expéditeur préféré.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

La page **CONFIGURATION système Options d'affichage** indique quel nœud d'administration est actuellement sélectionné comme expéditeur préféré. Le nœud d'administration principal est sélectionné par défaut.

Dans des conditions normales de fonctionnement du système, seul l'expéditeur préféré envoie les notifications suivantes :

- Messages AutoSupport
- Notifications SNMP
- E-mails d'alerte
- E-mails d'alarme (système hérité)

Cependant, tous les autres nœuds d'administration (expéditeurs de secours) surveillent l'expéditeur préféré. Si un problème est détecté, un expéditeur en attente peut également envoyer ces notifications.

Dans les cas suivants, l'expéditeur préféré et l'expéditeur de secours peuvent envoyer des notifications :

- Si les nœuds d'administration deviennent « en attente » les uns des autres, l'expéditeur préféré et les expéditeurs de secours tenteront d'envoyer des notifications, et plusieurs copies de notifications peuvent être reçues.
- Lorsqu'un expéditeur en veille détecte des problèmes avec l'expéditeur préféré et commence à envoyer des notifications, il est possible que l'expéditeur préféré puisse récupérer sa capacité à envoyer des notifications. Dans ce cas, des notifications en double peuvent être envoyées. L'expéditeur en attente

interrompt l'envoi des notifications lorsqu'il ne détecte plus d'erreurs sur l'expéditeur préféré.



Lorsque vous testez les notifications d'alarme et les messages AutoSupport, tous les nœuds Admin envoient l'e-mail de test. Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité.

Étapes

1. Sélectionnez **CONFIGURATION système Options d'affichage**.
2. Dans le menu Options d'affichage, sélectionnez **Options**.
3. Sélectionnez le nœud d'administration que vous souhaitez définir comme expéditeur préféré dans la liste déroulante.



Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	☐

Apply Changes

4. Sélectionnez **appliquer les modifications**.

Le nœud d'administration est défini comme l'expéditeur préféré des notifications.

Afficher l'état des notifications et les files d'attente

Le service Network Management System (NMS) sur les nœuds Admin envoie des notifications au serveur de messagerie. Vous pouvez afficher l'état actuel du service NMS ainsi que la taille de sa file d'attente de notifications sur la page moteur d'interface.

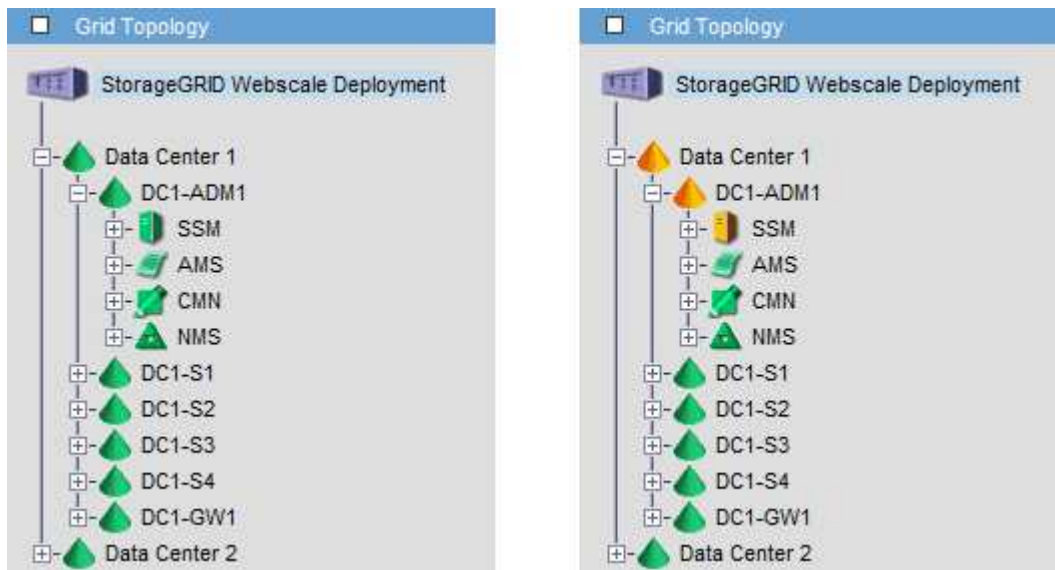
Pour accéder à la page moteur d'interface, sélectionnez **SUPPORT Outils topologie de grille**. Enfin, sélectionnez **site Admin Node NMS interface Engine**.

Les notifications sont traitées via la file d'attente de notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. En cas de problème (par exemple, une erreur de connexion réseau) et si le serveur de messagerie n'est pas disponible lors de la tentative d'envoi de la notification, une tentative de renvoi de la notification au serveur de messagerie se poursuit pendant une période de 60 secondes. Si la notification n'est pas envoyée au serveur de messagerie après 60 secondes, elle est supprimée de la file d'attente de notifications et une tentative d'envoi de la notification suivante dans la file d'attente est effectuée. Comme les notifications peuvent être supprimées de la file d'attente de notifications sans être envoyées, il est possible qu'une alarme puisse être déclenchée sans qu'une notification soit envoyée. Dans le cas où une notification est supprimée de la file d'attente sans être envoyée, l'alarme mineure EN MINUTES (état de notification par e-mail) est déclenchée.

Affichage des alarmes acquittées par les nœuds d'administration (système hérité)

Lorsque vous accusez réception d'une alarme sur un nœud d'administration, l'alarme acquittée n'est copiée sur aucun autre nœud d'administration. Comme les accusés de réception ne sont pas copiés sur d'autres nœuds d'administration, il est possible que l'arborescence de la topologie de grille ne soit pas identique pour chaque nœud d'administration.

Cette différence peut être utile lors de la connexion de clients Web. Les clients Web peuvent avoir différentes vues du système StorageGRID selon les besoins de l'administrateur.



Notez que les notifications sont envoyées depuis le nœud d'administration où l'accusé de réception a lieu.

Configurez l'accès client d'audit

Le nœud d'administration, via le service AMS (Audit Management System), consigne tous les événements système vérifiés dans un fichier journal disponible via le partage d'audit, qui est ajouté à chaque nœud d'administration lors de l'installation. Pour faciliter l'accès aux journaux d'audit, vous pouvez configurer l'accès des clients aux partages d'audit pour CIFS et NFS.

Le système StorageGRID utilise une reconnaissance positive pour éviter toute perte de messages d'audit avant qu'ils ne soient écrits dans le fichier journal. Un message reste placé dans la file d'attente d'un service jusqu'à ce que le service AMS ou un service de relais d'audit intermédiaire en ait reconnu le contrôle.

Pour plus d'informations, voir [Examiner les journaux d'audit](#).



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID. Si vous avez la possibilité d'utiliser CIFS ou NFS, choisissez NFS.

Configurer des clients d'audit pour CIFS

La procédure utilisée pour configurer un client d'audit dépend de la méthode d'authentification Windows Workgroup ou Windows Active Directory (AD). Lorsqu'il est

ajouté, le partage d'audit est automatiquement activé en tant que partage en lecture seule.



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Configurer les clients d'audit pour Workgroup

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.

4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Définissez l'authentification pour le groupe de travail Windows :

Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

- Entrez : `set-authentication`
- Lorsque vous êtes invité à installer Windows Workgroup ou Active Directory, entrez : `workgroup`
- Lorsque vous y êtes invité, entrez le nom du groupe de travail : `workgroup_name`
- Lorsque vous y êtes invité, créez un nom NetBIOS significatif : `netbios_name`

ou

Appuyez sur **entrée** pour utiliser le nom d'hôte du noeud d'administration comme nom NetBIOS.

Le script redémarre le serveur Samba et des modifications sont appliquées. Cela devrait prendre moins d'une minute. Une fois l'authentification définie, ajoutez un client d'audit.

- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

6. Ajouter un client d'audit :

- Entrez : `add-audit-share`



Le partage est automatiquement ajouté en lecture seule.

- Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user`
- Lorsque vous y êtes invité, entrez le nom d'utilisateur de l'audit : `audit_user_name`
- Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur d'audit : `password`
- Lorsque vous y êtes invité, saisissez à nouveau le même mot de passe pour le confirmer : `password`
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.



Il n'est pas nécessaire d'entrer un répertoire. Le nom du répertoire d'audit est prédéfini.

7. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez-les :

a. Entrez : `add-user-to-share`

Une liste numérotée des partages activés s'affiche.

b. Lorsque vous y êtes invité, entrez le numéro du partage audit-exportation : `share_number`

c. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user`

ou `group`

d. Lorsque vous y êtes invité, entrez le nom de l'utilisateur ou du groupe d'audit : `audit_user` or `audit_group`

e. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

f. Répétez ces sous-étapes pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

8. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Lorsque vous y êtes invité, appuyez sur **entrée**.

La configuration du client d'audit s'affiche.

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

9. Fermez l'utilitaire de configuration CIFS : `exit`

10. Démarrez le service Samba : `service smbd start`

11. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

ou

Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ce partage d'audit comme requis :

- a. Connectez-vous à distance au nœud d'administration d'un site :
 - i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour passer à la racine : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- b. Répétez les étapes pour configurer le partage d'audit pour chaque nœud d'administration supplémentaire.
- c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

12. Déconnectez-vous du shell de commande : `exit`

Configurer les clients d'audit pour Active Directory

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous disposez du nom d'utilisateur et du mot de passe CIFS Active Directory.
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Définissez l'authentification pour Active Directory : `set-authentication`

Dans la plupart des déploiements, vous devez définir l'authentification avant d'ajouter le client d'audit. Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

- Lorsque vous êtes invité à installer Workgroup ou Active Directory : `ad`
- À l'invite, entrez le nom du domaine AD (nom de domaine court).
- Indiquez l'adresse IP ou le nom d'hôte DNS du contrôleur de domaine.
- Lorsque vous y êtes invité, entrez le nom de domaine de domaine complet.

Utilisez des lettres majuscules.

- Lorsque vous êtes invité à activer la prise en charge de winbind, tapez **y**.

Winbind est utilisé pour résoudre les informations utilisateur et de groupe à partir des serveurs AD.

- Lorsque vous y êtes invité, entrez le nom NetBIOS.
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

6. Rejoindre le domaine :

- Si ce n'est pas déjà fait, démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`
- Rejoindre le domaine : `join-domain`
- Vous êtes invité à tester si le nœud d'administration est actuellement un membre valide du domaine. Si ce nœud d'administration n'a pas déjà rejoint le domaine, entrez : `no`
- Indiquez le nom d'utilisateur de l'administrateur lorsque vous y êtes invité :
`administrator_username`

où `administrator_username` Est le nom d'utilisateur CIFS Active Directory, pas le nom d'utilisateur StorageGRID.

- Lorsque vous y êtes invité, indiquez le mot de passe de l'administrateur : `administrator_password`

l'ont été `administrator_password` Est le nom d'utilisateur CIFS Active Directory, et non le mot de passe StorageGRID.

- f. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

7. Vérifiez que vous avez correctement joint le domaine :

- a. Rejoindre le domaine : `join-domain`

- b. Lorsque vous êtes invité à tester si le serveur est actuellement un membre valide du domaine, entrez :
`y`

Si vous recevez le message « rejoindre est OK », vous avez rejoint le domaine avec succès. Si vous n'obtenez pas cette réponse, essayez de définir l'authentification et de rejoindre à nouveau le domaine.

- c. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

8. Ajouter un client d'audit : `add-audit-share`

- a. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `user`

- b. Lorsque vous êtes invité à saisir le nom d'utilisateur de l'audit, entrez le nom d'utilisateur de l'audit.

- c. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

9. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez des utilisateurs supplémentaires : `add-user-to-share`

Une liste numérotée des partages activés s'affiche.

- a. Entrez le numéro du partage audit-exportation.

- b. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `group`

Vous êtes invité à entrer le nom du groupe d'audit.

- c. Lorsque vous êtes invité à entrer le nom du groupe d'audit, entrez le nom du groupe d'utilisateurs d'audit.

- d. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

- e. Répétez cette étape pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

10. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-filesystem.inc`

- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-custom-config.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-shares.inc`
- `rlimit_max` : augmentation de `rlimit_max` (1024) à la limite Windows minimale (16384)



Ne pas combiner le paramètre 'Security=ADS' avec le paramètre 'Password Server'.
(Par défaut, Samba détecte le bon DC à contacter automatiquement).

- Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

11. Fermez l'utilitaire de configuration CIFS : `exit`

12. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

ou

Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit comme requis :

- Connectez-vous à distance au nœud d'administration d'un site :
 - Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - Entrez la commande suivante pour passer à la racine : `su -`
 - Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
- Fermez la connexion du shell sécurisé distant au nœud d'administration : `exit`

13. Déconnectez-vous du shell de commande : `exit`

Ajoutez un utilisateur ou un groupe à un partage d'audit CIFS

Vous pouvez ajouter un utilisateur ou un groupe à un partage d'audit CIFS intégré à l'authentification AD.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

La procédure suivante concerne un partage d'audit intégré à l'authentification AD.



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config	

add-audit-share	set-authentication	validate-config	
enable-disable-share	set-netbios-name	help	
add-user-to-share	join-domain	exit	
remove-user-from-share	add-password-server		
modify-group	remove-password-server		
	add-wins-server		
	remove-wins-server		

5. Commencez à ajouter un utilisateur ou un groupe : `add-user-to-share`

Une liste numérotée de partages d'audit qui ont été configurés s'affiche.

6. Lorsque vous y êtes invité, entrez le numéro du partage d'audit (audit-export) : `audit_share_number`

On vous demande si vous souhaitez donner un accès à ce partage d'audit à un utilisateur ou à un groupe.

7. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user` ou `group`

8. Lorsque vous êtes invité à entrer le nom de l'utilisateur ou du groupe pour ce partage d'audit AD, entrez le nom.

L'utilisateur ou le groupe est ajouté en lecture seule pour le partage d'audit à la fois dans le système d'exploitation du serveur et dans le service CIFS. La configuration Samba est rechargée pour permettre à l'utilisateur ou au groupe d'accéder au partage du client d'audit.

9. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

10. Répétez ces étapes pour chaque utilisateur ou groupe ayant accès au partage d'audit.

11. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

- Impossible de trouver le fichier `/etc/samba/include/cifs-interfaces.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-filesystem.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-custom-config.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-shares.inc`
 - i. Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
 - ii. Lorsque vous y êtes invité, appuyez sur **entrée**.

12. Fermez l'utilitaire de configuration CIFS : `exit`

13. Déterminez si vous devez activer des partages d'audit supplémentaires, comme suit :

- Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
- Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :
 - i. Connectez-vous à distance au nœud d'administration d'un site :
 - A. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - C. Entrez la commande suivante pour passer à la racine : `su -`
 - D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
 - iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

14. Déconnectez-vous du shell de commande : `exit`

Supprimer un utilisateur ou un groupe d'un partage d'audit CIFS

Vous ne pouvez pas supprimer le dernier utilisateur ou groupe autorisé à accéder au partage d'audit.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec les mots de passe du compte racine (disponible dans LEDIT package).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

3. Commencez à supprimer un utilisateur ou un groupe : `remove-user-from-share`

Une liste numérotée des partages d'audit disponibles pour le nœud d'administration s'affiche. Le partage d'audit est étiqueté `audit-export`.

4. Entrez le numéro du partage d'audit : `audit_share_number`

5. Lorsque vous êtes invité à supprimer un utilisateur ou un groupe : `user` ou `group`

Une liste numérotée d'utilisateurs ou de groupes pour le partage d'audit s'affiche.

6. Entrez le numéro correspondant à l'utilisateur ou au groupe que vous souhaitez supprimer : `number`

Le partage d'audit est mis à jour et l'utilisateur ou le groupe n'est plus autorisé à accéder au partage d'audit. Par exemple :


```
Enabled shares
  1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
  1. audituser
  2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Fermez l'utilitaire de configuration CIFS : `exit`
8. Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, désactivez le partage d'audit sur chaque site selon les besoins.
9. Déconnectez-vous de chaque shell de commande une fois la configuration terminée : `exit`

Modifier un nom d'utilisateur ou de groupe de partage d'audit CIFS

Vous pouvez modifier le nom d'un utilisateur ou d'un groupe pour un partage d'audit CIFS en ajoutant un nouvel utilisateur ou un nouveau groupe, puis en supprimant l'ancien.

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Ajoutez un nouvel utilisateur ou un nouveau groupe portant le nom mis à jour au partage d'audit.
2. Supprimez l'ancien nom d'utilisateur ou de groupe.

Informations associées

- [Ajoutez un utilisateur ou un groupe à un partage d'audit CIFS](#)
- [Supprimer un utilisateur ou un groupe d'un partage d'audit CIFS](#)

Vérifier l'intégration de l'audit CIFS

Le partage d'audit est en lecture seule. Les fichiers journaux sont destinés à être lus par des applications informatiques et la vérification ne comprend pas l'ouverture d'un fichier. Il est considéré comme suffisant de vérifier que les fichiers journaux d'audit apparaissent dans une fenêtre de l'Explorateur Windows. Après vérification de la connexion, fermez toutes les fenêtres.

Configuration du client d'audit pour NFS

Le partage d'audit est automatiquement activé en tant que partage en lecture seule.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe root/admin (disponible dans LEDIT paquet).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).
- Le client d'audit utilise NFS version 3 (NFSv3).

Description de la tâche

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

Si des services ne sont pas répertoriés comme en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande. Appuyez sur **Ctrl+C**.

4. Démarrez l'utilitaire de configuration NFS. Entrez : `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share        | validate-config      |  
| enable-disable-share  | remove-ip-from-share   | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

5. Ajouter le client d'audit : `add-audit-share`

- a. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : `client_IP_address`
- b. Lorsque vous y êtes invité, appuyez sur **entrée**.

6. Si plusieurs clients d'audit sont autorisés à accéder au partage d'audit, ajoutez l'adresse IP de l'utilisateur supplémentaire : `add-ip-to-share`

- a. Entrez le numéro du partage d'audit : `audit_share_number`
- b. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le

partage d'audit : `client_IP_address`

c. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration NFS s'affiche.

d. Répétez ces sous-étapes pour chaque client d'audit supplémentaire ayant accès au partage d'audit.

7. Vérifiez éventuellement votre configuration.

a. Saisissez les informations suivantes : `validate-config`

Les services sont vérifiés et affichés.

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration NFS s'affiche.

c. Fermez l'utilitaire de configuration NFS : `exit`

8. Déterminez si vous devez activer des partages d'audit sur d'autres sites.

- Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
- Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :

i. Connectez-vous à distance au nœud d'administration du site :

A. Saisissez la commande suivante : `ssh admin@grid_node_IP`

B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

C. Entrez la commande suivante pour passer à la racine : `su -`

D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.

iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant. Entrez : `exit`

9. Déconnectez-vous du shell de commande : `exit`

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accordez l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage ou supprimez un client d'audit existant en supprimant son adresse IP.

Ajouter un client d'audit NFS à un partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accorder l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage d'audit.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

- Le client d'audit utilise NFS version 3 (NFSv3).

Étapes

1. Connectez-vous au nœud d'administration principal :

- Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour passer à la racine : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

Shares	Clients	Config
add-audit-share	add-ip-to-share	validate-config
enable-disable-share	remove-ip-from-share	refresh-config
		help
		exit

3. Entrez : `add-ip-to-share`

La liste des partages d'audit NFS activés sur le nœud d'administration s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Entrez le numéro du partage d'audit : `audit_share_number`

5. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : `client_IP_address`

Le client d'audit est ajouté au partage d'audit.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration NFS s'affiche.

7. Répétez les étapes pour chaque client d'audit qui doit être ajouté au partage d'audit.

8. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés.

- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration NFS s'affiche.

9. Fermez l'utilitaire de configuration NFS : `exit`

10. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, activez éventuellement ces partages d'audit si nécessaire :

- a. Connectez-vous à distance au nœud d'administration d'un site :
 - i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour passer à la racine : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
- c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

11. Déconnectez-vous du shell de commande : `exit`

Vérifier l'intégration de l'audit NFS

Après avoir configuré un partage d'audit et ajouté un client d'audit NFS, vous pouvez monter le partage client d'audit et vérifier que les fichiers sont disponibles à partir du partage d'audit.

Étapes

1. Vérifiez la connectivité (ou la variante du système client) à l'aide de l'adresse IP côté client du nœud d'administration hébergeant le service AMS. Entrez : `ping IP_address`

Vérifiez que le serveur répond, indiquant la connectivité.

2. Montez le partage d'audit en lecture seule à l'aide d'une commande appropriée au système d'exploitation client. Un exemple de commande Linux est (entrez sur une ligne) :

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export  
myAudit
```

Utilisez l'adresse IP du nœud d'administration hébergeant le service AMS et le nom de partage prédéfini pour le système d'audit. Le point de montage peut être n'importe quel nom sélectionné par le client (par exemple, `myAudit` dans la commande précédente).

3. Vérifiez que les fichiers sont disponibles à partir du partage d'audit. Entrez : `ls myAudit /*`

où `myAudit` est le point de montage du partage d'audit. Au moins un fichier journal doit être répertorié.

Supprimer un client d'audit NFS du partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Vous pouvez supprimer un client d'audit existant en supprimant son adresse IP.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).

- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

Vous ne pouvez pas supprimer la dernière adresse IP autorisée à accéder au partage d'audit.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

```

-----
| Shares                | Clients                | Config                |
-----
| add-audit-share       | add-ip-to-share       | validate-config      |
| enable-disable-share  | remove-ip-from-share  | refresh-config       |
|                       |                       | help                 |
|                       |                       | exit                 |
-----

```

3. Supprimez l'adresse IP du partage d'audit : `remove-ip-from-share`

Une liste numérotée de partages d'audit configurés sur le serveur s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Saisissez le numéro correspondant au partage d'audit : `audit_share_number`

Une liste numérotée d'adresses IP autorisées à accéder au partage d'audit s'affiche.

5. Saisissez le numéro correspondant à l'adresse IP que vous souhaitez supprimer.

Le partage d'audit est mis à jour et l'accès n'est plus autorisé à partir d'un client d'audit possédant cette adresse IP.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration NFS s'affiche.

7. Fermez l'utilitaire de configuration NFS : `exit`

8. Si votre déploiement StorageGRID est un déploiement de plusieurs sites de data Center avec des nœuds d'administration supplémentaires sur les autres sites, désactivez les partages d'audit suivants :

- a. Connectez-vous à distance au nœud d'administration de chaque site :

- i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour passer à la racine : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.
 - c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
9. Déconnectez-vous du shell de commande : `exit`

Modifier l'adresse IP d'un client d'audit NFS

Procédez comme suit si vous devez modifier l'adresse IP d'un client d'audit NFS.

Étapes

1. Ajouter une nouvelle adresse IP à un partage d'audit NFS existant.
2. Supprimez l'adresse IP d'origine.

Informations associées

- [Ajouter un client d'audit NFS à un partage d'audit](#)
- [Supprimer un client d'audit NFS du partage d'audit](#)

Gérer les nœuds d'archivage

Qu'est-ce qu'un nœud d'archivage

En option, chaque site de data Center StorageGRID peut être déployé avec un nœud d'archivage, ce qui vous permet de vous connecter à un système de stockage d'archivage externe ciblé, tel que Tivoli Storage Manager (TSM).

Le nœud d'archivage fournit une interface par le biais de laquelle vous pouvez cibler un système de stockage d'archives externe pour le stockage à long terme des données d'objet. Le nœud d'archivage surveille également cette connexion et le transfert des données d'objet entre le système StorageGRID et le système de stockage d'archives externes ciblé.

The screenshot shows the StorageGRID WebScale Deployment interface. On the left, the 'Grid Topology' pane displays a hierarchical view of the deployment, including Data Center 1, Data Center 2, and Data Center 3. Under Data Center 1, the ARC node (DC1-ARC1-98-165) is highlighted, showing its sub-components: SSM, Replication, Store, Retrieve, Target, Events, and Resources. On the right, the 'Overview' page for the selected ARC node is displayed. It includes tabs for Overview, Alarms, Reports, and Configuration. The Overview page shows the ARC State as 'Online' and ARC Status as 'No Errors'. It also displays the Tivoli Storage Manager State and Status, Store State and Status, Retrieve State and Status, and Inbound/Outbound Replication Status, all of which are 'Online' and 'No Errors'. Below this, the 'Node Information' section provides details about the device type (Archive Node), version (10.2.0), build (20150928.2133.a27b3ab), node ID (19002524), and site ID (10).

Après avoir configuré les connexions à la cible externe, vous pouvez configurer le nœud d'archivage pour optimiser les performances TSM, mettre un nœud d'archivage hors ligne lorsqu'un serveur TSM atteint sa capacité ou est indisponible, et configurer les paramètres de réplication et de récupération. Vous pouvez également définir des alarmes personnalisées pour le nœud d'archivage.

Les données d'objet qui ne peuvent pas être supprimées, mais qui ne sont pas régulièrement utilisées, peuvent à tout moment être déplacées hors des disques rotatifs d'un nœud de stockage, vers un stockage d'archivage externe tel que le cloud ou la bande. Cet archivage des données d'objet s'effectue via la configuration du nœud d'archivage d'un site de data Center, puis la configuration des règles ILM sur lesquelles ce nœud d'archivage est sélectionné comme « cible » pour les instructions de placement de contenu. Le nœud d'archivage ne gère pas les données d'objet archivées lui-même, ce qui est réalisé par le dispositif d'archivage externe.



Les métadonnées de l'objet ne sont pas archivées, mais restent sur les nœuds de stockage.

Qu'est-ce que le service ARC

Le service d'archivage (ARC) sur les nœuds d'archivage fournit l'interface de gestion que vous pouvez utiliser pour configurer les connexions au système de stockage d'archivage externe, comme les bandes via le middleware TSM.

Il s'agit du service ARC qui interagit avec un système de stockage d'archives externe, en envoyant des données d'objet pour le stockage secondaire et en effectuant des récupérations lorsqu'une application client demande un objet archivé. Lorsqu'une application client demande un objet archivé, un nœud de stockage demande les données de l'objet au service ARC. Le service ARC envoie une demande au système de stockage d'archives externe, qui récupère les données de l'objet demandé et les envoie au service ARC. Le service ARC vérifie les données de l'objet et les transfère au nœud de stockage, qui renvoie alors l'objet à l'application client requérant.

Les demandes de données d'objet archivées sur bande via un middleware TSM sont gérées pour optimiser les récupérations. Les demandes peuvent être commandées de façon à ce que les objets stockés dans l'ordre séquentiel sur bande soient demandés dans le même ordre séquentiel. Les demandes sont alors mises en file d'attente pour soumission à l'unité de stockage. En fonction du périphérique d'archivage, plusieurs demandes d'objets sur différents volumes peuvent être traitées simultanément.

Archivez vos données dans le cloud via l'API S3

Vous pouvez configurer un nœud d'archivage pour qu'il se connecte directement à Amazon Web Services (AWS) ou à tout autre système capable de s'interfacer avec le système StorageGRID via l'API S3.



Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archivage externe via l'API S3 a été remplacé par les pools de stockage cloud ILM, offrant ainsi plus de fonctionnalités. L'option **Cloud Tiering - simple Storage Service (S3)** est toujours prise en charge, mais vous préférez peut-être implémenter des pools de stockage cloud.

Si vous utilisez actuellement un nœud d'archivage avec l'option **Cloud Tiering - simple Storage Service (S3)**, envisagez de migrer vos objets vers un pool de stockage cloud. Reportez-vous aux instructions pour [Gestion des objets avec ILM](#).

Configurez les paramètres de connexion pour l'API S3

Si vous vous connectez à un nœud d'archivage à l'aide de l'interface S3, vous devez configurer les paramètres de connexion de l'API S3. Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne parvient pas à communiquer avec le système de stockage d'archives externe.



Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archivage externe via l'API S3 a été remplacé par les pools de stockage cloud ILM, offrant ainsi plus de fonctionnalités. L'option **Cloud Tiering - simple Storage Service (S3)** est toujours prise en charge, mais vous préférez peut-être implémenter des pools de stockage cloud.

Si vous utilisez actuellement un nœud d'archivage avec l'option **Cloud Tiering - simple Storage Service (S3)**, envisagez de migrer vos objets vers un pool de stockage cloud. Voir [Gestion des objets avec ILM](#).

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez créé un compartiment sur le système de stockage d'archivage cible :
 - Le compartiment est dédié à un seul nœud d'archivage. Il ne peut pas être utilisé par d'autres nœuds d'archivage ou d'autres applications.
 - La région du compartiment est sélectionnée pour votre emplacement.
 - Le compartiment doit être configuré avec une gestion des versions suspendue.
- La segmentation d'objet est activée et la taille de segment maximale est inférieure ou égale à 4.5 Gio (4,831,838,208 octets). Les demandes d'API S3 qui dépassent cette valeur échouent si S3 est utilisé comme système de stockage d'archivage externe.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node > ARC > Target**.
3. Sélectionnez **Configuration main**.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: ARC (98-127) - Target

Updated: 2015-09-24 15:48:22 PDT

Target Type:

Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:

name

Region:

Virginia or Pacific Northwest (us-east-1)

Endpoint:

https://10.10.10.123:8082

☐ Use AWS

Endpoint Authentication:

☐

Access Key:

ABCD123EFG45AB

Secret Access Key:

.....

Storage Class:

Standard (Default)

Apply Changes



- Sélectionnez **Cloud Tiering - simple Storage Service (S3)** dans la liste déroulante Type de cible.



Les paramètres de configuration ne sont pas disponibles tant que vous n'avez pas sélectionné de type cible.

- Configurez le compte de Tiering cloud (S3) via lequel le nœud d'archivage se connecte au système de stockage d'archivage externe cible compatible S3.

La plupart des champs de cette page sont explicites. La section suivante décrit les champs pour lesquels vous avez peut-être besoin d'aide.

- **Région** : disponible uniquement si **Use AWS** est sélectionné. La région que vous sélectionnez doit correspondre à la région du compartiment.
- **Endpoint** et **use AWS** : pour Amazon Web Services (AWS), sélectionnez **use AWS**. **Endpoint** est alors automatiquement renseigné avec une URL de point de terminaison en fonction des attributs Nom du compartiment et région. Par exemple :

`https://bucket.region.amazonaws.com`

Pour une cible non AWS, entrez l'URL du système hébergeant le compartiment, y compris le numéro de port. Par exemple :

`https://system.com:1080`

- **Authentification par point de terminaison** : activée par défaut. Si le réseau vers le système de stockage d'archives externe est approuvé, vous pouvez désélectionner la case à cocher pour désactiver le certificat SSL de point final et la vérification du nom d'hôte pour le système de stockage

d'archives externe cible. Si une autre instance d'un système StorageGRID est le périphérique de stockage d'archives cible et que le système est configuré avec des certificats signés publiquement, vous pouvez maintenir la case à cocher sélectionnée.

- **Classe de stockage** : sélectionnez **Standard (par défaut)** pour le stockage normal. Sélectionnez **réduction de redondance** uniquement pour les objets qui peuvent être facilement recréés. **Redondance réduite** fournit un stockage moins coûteux et moins fiable. Si le système de stockage d'archives cible est une autre instance du système StorageGRID, **Storage Class** contrôle le nombre de copies intermédiaires de l'objet à l'entrée sur le système cible, si la double validation est utilisée lors de l'ingestion d'objets.

6. Sélectionnez **appliquer les modifications**.

Les paramètres de configuration spécifiés sont validés et appliqués à votre système StorageGRID. Une fois configurée, la cible ne peut plus être modifiée.

Modifiez les paramètres de connexion de l'API S3

Une fois que le nœud d'archivage est configuré pour se connecter à un système de stockage d'archives externe via l'API S3, vous pouvez modifier certains paramètres en cas de modification de la connexion.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si vous modifiez le compte Cloud Tiering (S3), vous devez vous assurer que les identifiants d'accès utilisateur ont un accès en lecture/écriture au compartiment, y compris tous les objets précédemment ingérées par le nœud d'archivage vers le compartiment.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC cible**.
3. Sélectionnez **Configuration main**.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: ARC (98-127) - Target

Updated: 2015-09-24 15:48:22 PDT

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:	name		
Region:	Virginia or Pacific Northwest (us-east-1)		
Endpoint:	https://10.10.10.123:8082	☐	Use AWS
Endpoint Authentication:	☐		
Access Key:	ABCD123EFG45AB		
Secret Access Key:	••••••		
Storage Class:	Standard (Default)		

Apply Changes 

4. Modifiez les informations de compte si nécessaire.

Si vous modifiez la classe de stockage, les nouvelles données d'objet sont stockées avec la nouvelle classe de stockage. Un objet existant reste stocké sous la classe de stockage définie lors de l'ingestion.



Le nom du compartiment, la région et le point de terminaison utilisent les valeurs AWS et ne peuvent pas être modifiés.

5. Sélectionnez **appliquer les modifications**.

Modifiez l'état du service NetApp Cloud Tiering

Vous pouvez contrôler la capacité de lecture et d'écriture du nœud d'archivage sur le système de stockage d'archives externe ciblé qui se connecte via l'API S3 en modifiant l'état du service de Tiering cloud.

Ce dont vous avez besoin

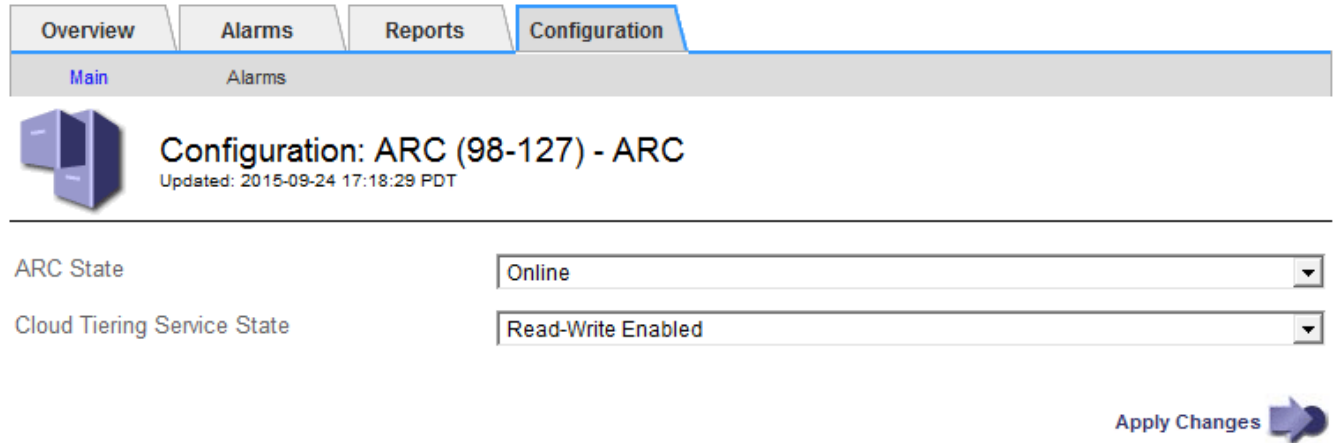
- Vous devez être connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le nœud d'archivage doit être configuré.

Description de la tâche

Vous pouvez mettre le nœud d'archivage hors ligne en changeant l'état du service de Tiering cloud sur **Read-Write Disabled**.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC**.
3. Sélectionnez **Configuration main**.



The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below it, the 'Main' sub-tab is active. The page title is 'Configuration: ARC (98-127) - ARC' with a timestamp 'Updated: 2015-09-24 17:18:29 PDT'. There are two dropdown menus: 'ARC State' set to 'Online' and 'Cloud Tiering Service State' set to 'Read-Write Enabled'. An 'Apply Changes' button with a right-pointing arrow is at the bottom right.

4. Sélectionnez un **Cloud Tiering Service State**.
5. Sélectionnez **appliquer les modifications**.

Réinitialisez le nombre d'échecs de stockage pour la connexion API S3

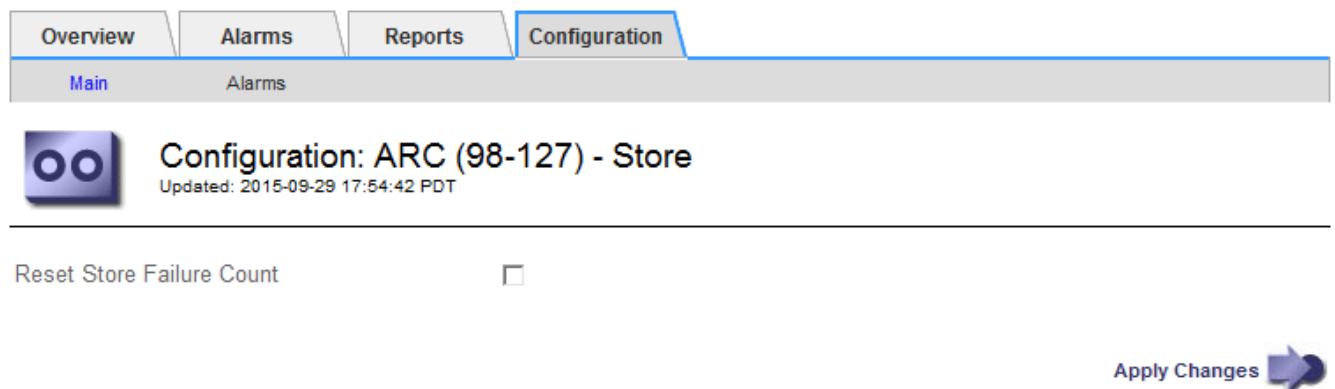
Si votre nœud d'archivage se connecte à un système de stockage d'archives via l'API S3, vous pouvez réinitialiser le nombre d'échecs de stockage, qui peut être utilisé pour effacer l'alarme ARVF (échecs de stockage).

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC Store**.
3. Sélectionnez **Configuration main**.



The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below it, the 'Main' sub-tab is active. The page title is 'Configuration: ARC (98-127) - Store' with a timestamp 'Updated: 2015-09-29 17:54:42 PDT'. There is a checkbox labeled 'Reset Store Failure Count'. An 'Apply Changes' button with a right-pointing arrow is at the bottom right.

4. Sélectionnez **Réinitialiser le nombre d'échecs de stockage**.

5. Sélectionnez **appliquer les modifications**.

L'attribut Store Failures se réinitialise sur zéro.

Migrer des objets depuis Cloud Tiering - S3 vers un pool de stockage cloud

Si vous utilisez actuellement la fonctionnalité **Cloud Tiering - simple Storage Service (S3)** pour hiérarchiser les données d'objet vers un compartiment S3, envisagez de migrer vos objets vers un pool de stockage cloud. Les pools de stockage cloud offrent une approche évolutive qui tire parti de tous les nœuds de stockage dans votre système StorageGRID.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Des objets sont déjà stockés dans le compartiment S3 configuré pour le Tiering dans le cloud.



Avant de migrer les données d'objet, contactez votre ingénieur commercial NetApp pour comprendre et gérer les coûts éventuels associés.

Description de la tâche

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Toutefois, si les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment S3 externe.

Avant de migrer les objets depuis Cloud Tiering - S3 vers un pool de stockage cloud, vous devez d'abord créer un compartiment S3, puis créer le pool de stockage cloud dans StorageGRID. Vous pouvez ensuite créer une nouvelle règle ILM et remplacer la règle ILM utilisée pour stocker les objets dans le compartiment Cloud Tiering par une règle ILM clonée qui stocke les mêmes objets dans le pool de stockage cloud.



Lorsque des objets sont stockés dans un pool de stockage cloud, des copies de ces objets ne peuvent pas également être stockées dans StorageGRID. Si la règle ILM que vous utilisez actuellement pour Cloud Tiering est configurée pour stocker les objets en même temps, déterminez si vous souhaitez toujours effectuer cette migration facultative, car elle sera perdue. Si vous continuez cette migration, vous devez créer de nouvelles règles au lieu de cloner les règles existantes.

Étapes

1. Création d'un pool de stockage cloud.

Utilisez un nouveau compartiment S3 pour le pool de stockage cloud afin de garantir que celui-ci contient uniquement les données gérées par le pool de stockage cloud.

2. Recherchez toutes les règles ILM de la règle ILM active qui entraîne le stockage des objets dans le compartiment de NetApp Cloud Tiering.

3. Clonez chacune de ces règles.

4. Dans les règles clonées, modifiez l'emplacement de placement dans le nouveau pool de stockage cloud.

5. Enregistrez les règles clonées.

6. Création d'une nouvelle règle qui utilise les nouvelles règles
7. Simuler et activer la nouvelle règle.

Lorsque la nouvelle règle est activée et que l'évaluation ILM est effectuée, les objets sont déplacés du compartiment S3 configuré pour NetApp Cloud Tiering vers le compartiment S3 configuré pour le pool de stockage cloud. L'espace utilisable sur la grille n'est pas affecté. Une fois les objets déplacés vers le pool de stockage cloud, ils sont supprimés du compartiment de NetApp Cloud Tiering.

Informations associées

[Gestion des objets avec ILM](#)

Archivez vos données sur bande via le logiciel médiateur TSM

Vous pouvez configurer un nœud d'archivage pour qu'il cible un serveur Tivoli Storage Manager (TSM) qui fournit une interface logique permettant de stocker et de récupérer des données d'objet sur des unités de stockage à accès aléatoire ou séquentiel, y compris des bibliothèques de bandes.

Le service ARC du nœud d'archivage sert de client au serveur TSM, utilisant Tivoli Storage Manager comme logiciel médiateur pour communiquer avec le système de stockage d'archives.

Cours de gestion TSM

Les classes de gestion définies par le middleware TSM décrivent le fonctionnement des opérations de sauvegarde et d'archivage de TSM's et peuvent être utilisées pour spécifier les règles du contenu appliqué par le serveur TSM. Ces règles fonctionnent indépendamment de la politique ILM du système StorageGRID et doivent rester cohérentes avec StorageGRID la condition que les objets soient stockés de manière permanente et soient toujours disponibles pour la récupération par le nœud d'archivage. Une fois les données d'objet envoyées à un serveur TSM par le nœud d'archivage, les règles de cycle de vie et de conservation TSM sont appliquées pendant que les données de l'objet sont stockées sur bande gérée par le serveur TSM.

La classe de gestion TSM est utilisée par le serveur TSM pour appliquer des règles pour l'emplacement ou la conservation des données après que les objets soient envoyés au serveur TSM par le nœud d'archivage. Par exemple, les objets identifiés comme sauvegardes de bases de données (contenu temporaire pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données d'application (contenu fixe qui doit être conservé indéfiniment).

Configurer les connexions au middleware TSM

Avant que le nœud d'archivage puisse communiquer avec le middleware Tivoli Storage Manager (TSM), vous devez configurer un certain nombre de paramètres.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne peut pas communiquer avec Tivoli Storage Manager.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC cible**.
3. Sélectionnez **Configuration main**.

Overview Alarms Reports **Configuration**

Main Alarms

Configuration: ARC (DC1-ARC1-98-165) - Target
Updated: 2015-09-28 09:56:36 PDT

Target Type: Tivoli Storage Manager (TSM)

Tivoli Storage Manager State: Online

Target (TSM) Account

Server IP or Hostname: 10.10.10.123

Server Port: 1500

Node Name: ARC-USER

User Name: arc-user

Password: ••••••

Management Class: sg-mgmtclass

Number of Sessions: 2

Maximum Retrieve Sessions: 1

Maximum Store Sessions: 1

Apply Changes

4. Dans la liste déroulante **Type cible**, sélectionnez **Tivoli Storage Manager (TSM)**.
5. Pour l'état **Tivoli Storage Manager**, sélectionnez **Offline** pour empêcher les récupérations du serveur middleware TSM.

Par défaut, l'état Tivoli Storage Manager est défini sur en ligne, ce qui signifie que le noeud d'archivage peut récupérer des données d'objet à partir du serveur middleware TSM.

6. Complétez les informations suivantes :

- **IP ou Nom d'hôte du serveur** : spécifiez l'adresse IP ou le nom de domaine complet du serveur middleware TSM utilisé par le service ARC. L'adresse IP par défaut est 127.0.0.1.
- **Port serveur** : spécifiez le numéro de port sur le serveur middleware TSM auquel le service ARC se connectera. La valeur par défaut est 1500.
- **Nom du noeud** : spécifiez le nom du noeud d'archive. Vous devez entrer le nom (utilisateur d'arc) que vous avez enregistré sur le serveur middleware TSM.
- **Nom d'utilisateur** : spécifiez le nom d'utilisateur utilisé par le service ARC pour se connecter au serveur TSM. Entrez le nom d'utilisateur par défaut (utilisateur d'arc) ou l'utilisateur administratif spécifié pour le noeud d'archivage.
- **Mot de passe** : Indiquez le mot de passe utilisé par le service ARC pour se connecter au serveur TSM.

- **Classe de gestion** : spécifiez la classe de gestion par défaut à utiliser si une classe de gestion n'est pas spécifiée lors de l'enregistrement de l'objet sur le système StorageGRID ou si la classe de gestion spécifiée n'est pas définie sur le serveur middleware TSM.
- **Nombre de sessions** : spécifiez le nombre de lecteurs de bande sur le serveur middleware TSM dédié au nœud d'archivage. Le nœud d'archivage crée simultanément un maximum d'une session par point de montage et un petit nombre de sessions supplémentaires (moins de cinq).

Vous devez modifier cette valeur pour qu'elle soit identique à la valeur définie pour MAXNUMMP (nombre maximal de points de montage) lorsque le nœud d'archivage a été enregistré ou mis à jour. (Dans la commande REGISTER, la valeur par défaut de MAXNUMMP utilisée est 1, si aucune valeur n'est définie.)

Vous devez également modifier la valeur de MAXSESSIONS pour le serveur TSM à un nombre au moins aussi important que le nombre de sessions défini pour le service ARC. La valeur par défaut de MAXSESSIONS sur le serveur TSM est 25.

- **Nombre maximal de sessions de récupération** : spécifiez le nombre maximal de sessions que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations de récupération. Dans la plupart des cas, la valeur appropriée est le nombre de sessions moins le nombre maximal de sessions en magasin. Si vous devez partager un lecteur de bande pour le stockage et la récupération, spécifiez une valeur égale au nombre de sessions.
- **Nombre maximal de sessions de stockage** : spécifiez le nombre maximal de sessions simultanées que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations d'archivage.

Cette valeur doit être définie sur une seule, sauf lorsque le système de stockage d'archives ciblé est plein et que seules les récupérations peuvent être effectuées. Définissez cette valeur sur zéro pour utiliser toutes les sessions pour les récupérations.

7. Sélectionnez **appliquer les modifications**.

Optimisez un nœud d'archivage pour les sessions middleware TSM

Vous pouvez optimiser les performances d'un nœud d'archivage qui se connecte à Tivoli Server Manager (TSM) en configurant les sessions du nœud d'archivage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

En général, le nombre de sessions simultanées que le nœud d'archivage a ouvertes au serveur middleware TSM est défini sur le nombre de lecteurs de bande que le serveur TSM a dédiés au nœud d'archivage. Un lecteur de bande est alloué au stockage tandis que le reste est alloué à la récupération. Toutefois, lorsqu'un nœud de stockage est en cours de reconstruction à partir de copies de nœud d'archivage ou que le nœud d'archivage fonctionne en mode lecture seule, vous pouvez optimiser les performances du serveur TSM en définissant le nombre maximal de sessions d'extraction à identique au nombre de sessions simultanées. Il en résulte que tous les disques peuvent être utilisés simultanément pour la récupération et, au plus, un de ces lecteurs peut également être utilisé pour le stockage, le cas échéant.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC cible**.

- Sélectionnez **Configuration main**.
- Modifier **nombre maximal de sessions de récupération** pour être le même que **nombre de sessions**.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: ARC (DC1-ARC1-98-165) - Target

Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager (TSM)

Tivoli Storage Manager State:

Online

Target (TSM) Account

Server IP or Hostname:

10.10.10.123

Server Port:

1500

Node Name:

ARC-USER

User Name:

arc-user

Password:

••••••

Management Class:

sg-mgmtclass

Number of Sessions:

2

Maximum Retrieve Sessions:

2

Maximum Store Sessions:

1

Apply Changes



- Sélectionnez **appliquer les modifications**.

Configurer l'état d'archivage et les compteurs pour TSM

Si votre nœud d'archivage se connecte à un serveur middleware TSM, vous pouvez configurer l'état du magasin d'archives d'un nœud d'archivage sur en ligne ou hors ligne. Vous pouvez également désactiver le magasin d'archives lors du premier démarrage du nœud d'archivage ou réinitialiser le nombre d'échecs en cours de suivi pour l'alarme associée.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

- Sélectionnez **SUPPORT > Outils > topologie de grille**.
- Sélectionnez **Archive Node ARC Store**.
- Sélectionnez **Configuration main**.

OverviewAlarmsReportsConfiguration

MainAlarms



Configuration: ARC (DC1-ARC1-98-165) - Store

Updated: 2015-09-29 17:10:12 PDT

Store State

Online

Archive Store Disabled on Startup

☐

Reset Store Failure Count

☐

Apply Changes

4. Modifiez les paramètres suivants, si nécessaire :

- État du stockage : définissez l'état du composant sur :
 - En ligne : le nœud d'archivage est disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archivage.
 - Hors ligne : le nœud d'archivage n'est pas disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archives.
- Magasin d'archives désactivé au démarrage : lorsque cette option est sélectionnée, le composant stockage d'archives reste en lecture seule lors du redémarrage. Utilisé pour désactiver de manière persistante le stockage vers le système cible de stockage d'archives. Utile lorsque le système de stockage d'archives ciblé ne peut pas accepter de contenu.
- Réinitialiser le nombre d'échecs du magasin : réinitialisez le compteur pour les échecs du magasin. Il peut être utilisé pour effacer l'alarme ARVF (Store Failure).

5. Sélectionnez **appliquer les modifications**.

Informations associées

[Gérer un nœud d'archivage lorsque le serveur TSM atteint sa capacité](#)

Gérer un nœud d'archivage lorsque le serveur TSM atteint sa capacité

Le serveur TSM n'a aucun moyen d'informer le nœud d'archivage lorsque la base de données TSM ou le stockage des supports d'archivage gérés par le serveur TSM atteint sa capacité maximale. Cette situation peut être évitée grâce à la surveillance proactive du serveur TSM.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

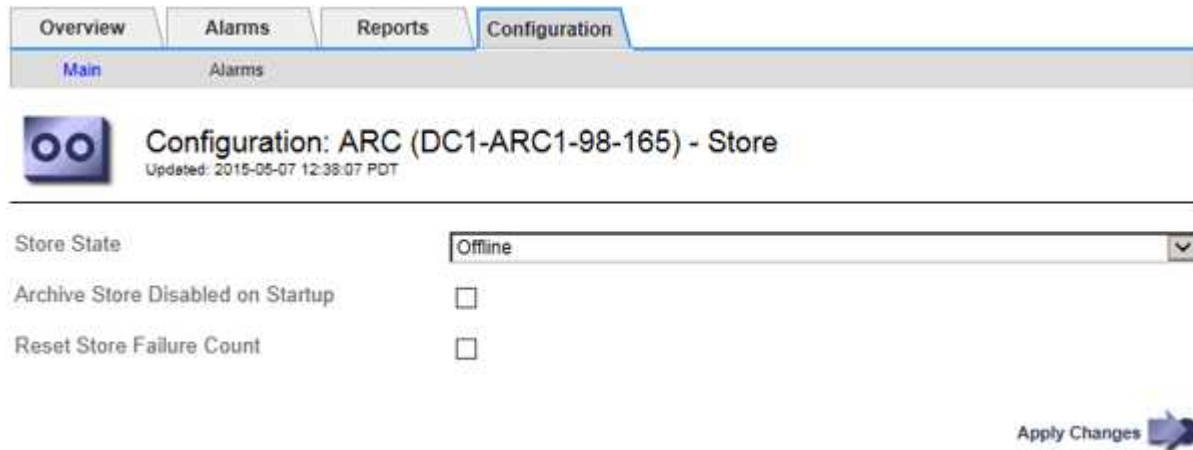
Le nœud d'archivage continue à accepter les données d'objet pour le transfert vers le serveur TSM une fois que le serveur TSM a arrêté d'accepter le nouveau contenu. Ce contenu ne peut pas être écrit sur un support géré par le serveur TSM. Une alarme est déclenchée si cela se produit.

Empêcher le service ARC d'envoyer du contenu au serveur TSM

Pour empêcher le service ARC d'envoyer du contenu supplémentaire au serveur TSM, vous pouvez mettre le nœud d'archivage hors ligne en mettant hors ligne son composant **ARC Store**. Cette procédure peut également être utile pour empêcher les alarmes lorsque le serveur TSM n'est pas disponible pour la maintenance.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC Store**.
3. Sélectionnez **Configuration main**.



4. Définissez **Etat du magasin** sur *Offline*.
5. Sélectionnez **Archive Store Disabled au démarrage**.
6. Sélectionnez **appliquer les modifications**.

Définissez le nœud d'archivage sur lecture seule si le middleware TSM atteint sa capacité

Si le serveur middleware TSM cible atteint sa capacité, le nœud d'archivage peut être optimisé pour effectuer uniquement des récupérations.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC cible**.
3. Sélectionnez **Configuration main**.
4. Modifiez le nombre maximal de sessions de récupération pour qu'il soit identique au nombre de sessions simultanées répertoriées dans nombre de sessions.
5. Définissez le nombre maximum de sessions de stockage sur 0.



Il n'est pas nécessaire de modifier le nombre maximal de sessions de stockage sur 0 si le nœud d'archivage est en lecture seule. Les sessions de magasin ne seront pas créées.

6. Sélectionnez **appliquer les modifications**.

Configurer les paramètres de récupération du nœud d'archivage

Vous pouvez configurer les paramètres de récupération d'un nœud d'archivage pour définir l'état en ligne ou hors ligne, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC Retrieve**.
3. Sélectionnez **Configuration main**.

Overview Alarms Reports **Configuration**

Main Alarms

Configuration: ARC (DC1-ARC1-98-165) - Retrieve
Updated: 2015-05-07 12:24:45 PDT

Retrieve State: Online

Reset Request Failure Count: ☐

Reset Verification Failure Count: ☐

Apply Changes

4. Modifiez les paramètres suivants, si nécessaire :
 - **Récupérer l'état** : définissez l'état du composant sur :
 - En ligne : le nœud de grille est disponible pour récupérer les données d'objet à partir du périphérique de support d'archivage.
 - Hors ligne : le nœud grid n'est pas disponible pour récupérer les données d'objet.
 - Réinitialiser le nombre d'échecs de la demande : cochez la case pour réinitialiser le compteur pour les échecs de la demande. Il peut être utilisé pour effacer l'alarme ARRF (demandes d'échecs).
 - Réinitialiser le nombre d'échecs de vérification : cochez cette case pour réinitialiser le compteur d'échecs de vérification sur les données d'objet récupérées. Il peut être utilisé pour effacer l'alarme ARRV (échecs de vérification).
5. Sélectionnez **appliquer les modifications**.

Configurer la réplication du nœud d'archivage

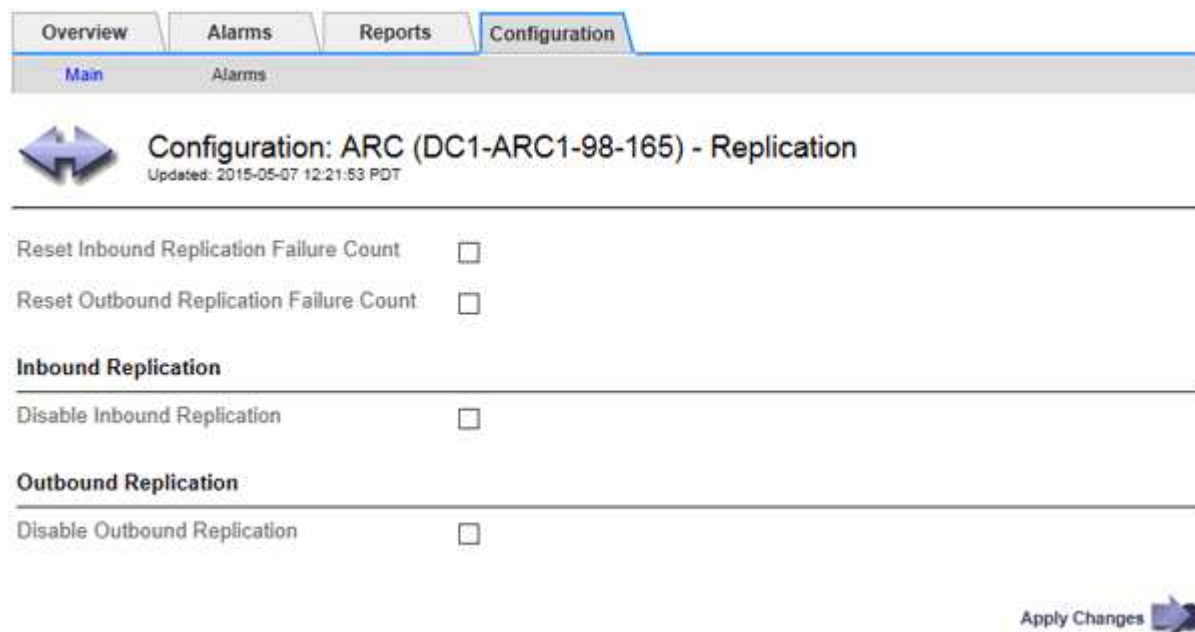
Vous pouvez configurer les paramètres de réplication d'un nœud d'archivage et désactiver la réplication entrante et sortante, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT > Outils > topologie de grille**.
2. Sélectionnez **Archive Node ARC Replication**.
3. Sélectionnez **Configuration main**.



The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below the tabs, there is a sub-header 'Configuration: ARC (DC1-ARC1-98-165) - Replication' with a timestamp 'Updated: 2015-05-07 12:21:53 PDT'. The main content area contains several configuration options, each with a checkbox:

- Reset Inbound Replication Failure Count ☐
- Reset Outbound Replication Failure Count ☐
- Inbound Replication**
 - Disable Inbound Replication ☐
- Outbound Replication**
 - Disable Outbound Replication ☐

At the bottom right, there is an 'Apply Changes' button with a right-pointing arrow icon.

4. Modifiez les paramètres suivants, si nécessaire :

- **Réinitialiser le nombre d'échecs de réplication entrant** : sélectionnez cette option pour réinitialiser le compteur pour les échecs de réplication entrants. Cette fonction permet d'effacer l'alarme RRF (Replications entrantes — FAILED).
- **Réinitialiser le nombre d'échecs de réplication sortante** : sélectionnez cette option pour réinitialiser le compteur des échecs de réplication sortants. Cette fonction permet d'effacer l'alarme RORF (réplications sortantes — en échec).
- **Désactiver la réplication entrante** : sélectionnez cette option pour désactiver la réplication entrante dans le cadre d'une procédure de maintenance ou de test. Laisser effacé pendant le fonctionnement normal.

Lorsque la réplication entrante est désactivée, les données d'objet peuvent être extraites du service ARC pour la réplication vers d'autres emplacements du système StorageGRID, mais les objets ne peuvent pas être répliqués vers ce service ARC à partir d'autres emplacements du système. Le service ARC est en lecture seule.

- **Désactiver la réplication sortante** : cochez cette case pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal.

Lorsque la réplication sortante est désactivée, les données d'objet peuvent être copiées vers ce service ARC afin de satisfaire aux règles ILM, mais les données d'objet ne peuvent pas être récupérées à partir du service ARC pour être copiées vers d'autres emplacements du système StorageGRID. Le service ARC est en écriture uniquement.

5. Sélectionnez **appliquer les modifications**.

Définissez les alarmes personnalisées pour le nœud d'archivage

Vous devez établir des alarmes personnalisées pour les attributs ARQL et ARRL utilisés pour surveiller la vitesse et l'efficacité de la récupération des données d'objet à partir du système de stockage d'archives par le nœud d'archivage.

- ARQL : longueur moyenne de la file d'attente. Durée moyenne, en microsecondes, de la mise en file d'attente des données de cet objet pour la récupération à partir du système de stockage d'archivage.
- ARRL : latence moyenne de la requête. Temps moyen, en microsecondes, requis par le nœud d'archivage pour récupérer les données d'objet à partir du système de stockage d'archivage.

Les valeurs acceptables pour ces attributs dépendent de la configuration et de l'utilisation du système de stockage d'archives. (Allez à **ARC Retrieve vue d'ensemble main**.) Les valeurs définies pour les délais de requête et le nombre de sessions disponibles pour les demandes de récupération sont particulièrement influentes.

Une fois l'intégration terminée, surveillez les récupérations de données d'objet du nœud d'archivage pour établir des valeurs pour les temps de récupération normaux et la longueur de file d'attente. Ensuite, créez des alarmes personnalisées pour ARQL et ARRL qui se déclencheront en cas de condition de fonctionnement anormale. Voir [Surveiller et résoudre les problèmes](#).

Intégrez Tivoli Storage Manager

Configuration et fonctionnement du nœud d'archivage

Votre système StorageGRID gère le nœud d'archivage comme un emplacement dans lequel les objets sont stockés indéfiniment et sont toujours accessibles.

À l'ingestion d'un objet, des copies sont effectuées dans tous les emplacements nécessaires, y compris les nœuds d'archivage, en fonction des règles de gestion du cycle de vie des informations (ILM) définies pour votre système StorageGRID. Le nœud d'archivage agit comme un client sur un serveur TSM, et les bibliothèques clientes TSM sont installées sur le nœud d'archivage par le processus d'installation du logiciel StorageGRID. Les données d'objet dirigées vers le nœud d'archivage pour le stockage sont enregistrées directement sur le serveur TSM au moment de leur réception. Le nœud d'archivage n'exécute pas les données d'objet avant de les enregistrer sur le serveur TSM, ni l'agrégation d'objets. Cependant, le nœud d'archivage peut envoyer plusieurs copies au serveur TSM en une seule transaction lorsque le taux de données le garantit.

Une fois que le nœud d'archivage enregistre les données d'objet sur le serveur TSM, les données d'objet sont gérées par le serveur TSM à l'aide de ses politiques de cycle de vie/rétention. Ces règles de conservation doivent être définies pour être compatibles avec le fonctionnement du nœud d'archivage. En d'autres termes, les données d'objet enregistrées par le nœud d'archivage doivent être stockées indéfiniment et doivent toujours être accessibles par le nœud d'archivage, à moins qu'elles ne soient supprimées par le nœud d'archivage.

Il n'y a aucune connexion entre les règles ILM du système StorageGRID et les politiques de cycle de vie/conservation du serveur TSM. Chaque système fonctionne de manière indépendante ; cependant, lorsque chaque objet est ingéré dans le système StorageGRID, vous pouvez lui attribuer une classe de gestion TSM. Cette classe de gestion est transmise au serveur TSM avec les données d'objet. L'affectation de classes de gestion à différents types d'objets vous permet de configurer le serveur TSM pour placer les données d'objet dans différents pools de stockage, ou d'appliquer différentes règles de migration ou de conservation, le cas échéant. Par exemple, les objets identifiés comme sauvegardes de bases de données (le contenu temporaire

pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données applicatives (contenu fixe qui doit être conservé indéfiniment).

Le nœud d'archivage peut être intégré à un nouveau serveur TSM ou à un serveur TSM existant ; il ne nécessite pas de serveur TSM dédié. Les serveurs TSM peuvent être partagés avec d'autres clients, à condition que la taille du serveur TSM soit adaptée à la charge maximale attendue. TSM doit être installé sur un serveur ou une machine virtuelle distincte du nœud d'archivage.

Il est possible de configurer plusieurs nœuds d'archivage pour écrire sur le même serveur TSM. Cependant, cette configuration n'est recommandée que si les nœuds d'archivage écrivent différents ensembles de données sur le serveur TSM. Il n'est pas recommandé de configurer plusieurs nœuds d'archivage pour écrire sur le même serveur TSM lorsque chaque nœud d'archivage écrit des copies des mêmes données d'objet dans l'archive. Dans ce dernier scénario, les deux copies sont soumises à un point de défaillance unique (le serveur TSM), pour les copies redondantes et indépendantes des données d'objet.

Les nœuds d'archivage n'utilisent pas le composant HSM (Hierarchical Storage Management) de TSM.

Bonnes pratiques pour la configuration

Lorsque vous dimensionnez et configurez votre serveur TSM, il existe les meilleures pratiques que vous devez appliquer pour l'optimiser afin qu'il fonctionne avec le nœud d'archivage.

Lors du dimensionnement et de la configuration du serveur TSM, il est important de prendre en compte les facteurs suivants :

- Comme le nœud d'archivage ne agrège pas les objets avant de les enregistrer sur le serveur TSM, la base de données TSM doit être dimensionnée pour contenir les références à tous les objets qui seront écrits sur le nœud d'archivage.
- Le logiciel Archive Node ne peut pas tolérer la latence impliquée dans l'écriture d'objets directement sur bande ou sur un autre support amovible. Par conséquent, le serveur TSM doit être configuré avec un pool de stockage sur disque pour le stockage initial des données sauvegardées par le nœud d'archivage chaque fois que des supports amovibles sont utilisés.
- Vous devez configurer les règles de conservation TSM pour utiliser la conservation basée sur les événements. Le nœud d'archivage ne prend pas en charge les politiques de conservation TSM basées sur la création. Utilisez les paramètres recommandés suivants de `retmin=0` et `retver=0` dans la stratégie de rétention (ce qui indique que la rétention commence lorsque le nœud d'archivage déclenche un événement de rétention et est conservé pendant 0 jours après cela). Toutefois, ces valeurs pour le `retmin` et le `retver` sont facultatives.

Le pool de disques doit être configuré pour migrer les données vers le pool de bandes (c'est-à-dire que le pool de bandes doit être le `NXTSTGPOOL` du pool de disques). Le pool de bandes ne doit pas être configuré en tant que pool de copies du pool de disques avec écriture simultanée sur les deux pools (c'est-à-dire que le pool de bandes ne peut pas être `COPYSTGPOOL` pour le pool de disques). Pour créer des copies hors ligne des bandes contenant les données du nœud d'archivage, configurez le serveur TSM avec un deuxième pool de bandes qui est un pool de copies du pool de bandes utilisé pour les données du nœud d'archivage.

Terminez la configuration du nœud d'archivage

Le nœud d'archivage ne fonctionne pas après avoir terminé le processus d'installation. Avant que le système StorageGRID puisse enregistrer des objets sur le nœud d'archivage TSM, vous devez terminer l'installation et la configuration du serveur TSM et configurer le nœud d'archivage pour qu'il communique avec le serveur TSM.

Si nécessaire, reportez-vous à la documentation IBM suivante lorsque vous préparez votre serveur TSM pour l'intégration au nœud d'archivage d'un système StorageGRID :

- ["Guide d'installation et d'utilisation des pilotes de périphérique de bande IBM"](#)
- ["Référence de programmation des pilotes de périphériques de bande IBM"](#)

Installez un nouveau serveur TSM

Vous pouvez intégrer le nœud d'archivage à un nouveau serveur TSM ou à un serveur TSM existant. Si vous installez un nouveau serveur TSM, suivez les instructions de la documentation TSM pour terminer l'installation.



Un nœud d'archive ne peut pas être co-hébergé avec un serveur TSM.

Configurer le serveur TSM

Cette section comprend des exemples d'instructions pour préparer un serveur TSM conformément aux meilleures pratiques TSM.

Les instructions suivantes vous guident tout au long du processus :

- Définition d'un pool de stockage sur disque et d'un pool de stockage sur bandes (le cas échéant) sur le serveur TSM
- Définition d'une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage et enregistrement d'un nœud pour utiliser cette stratégie de domaine

Ces instructions sont fournies à titre indicatif uniquement. Elles ne sont pas destinées à remplacer la documentation TSM ou à fournir des instructions complètes et complètes adaptées à toutes les configurations. Des instructions spécifiques à un déploiement doivent être fournies par un administrateur TSM qui connaît à la fois vos exigences détaillées et la documentation complète de TSM Server.

Définir les pools de stockage sur bande et sur disque TSM

Le nœud d'archivage écrit dans un pool de stockage sur disque. Pour archiver du contenu sur bande, vous devez configurer le pool de stockage sur disque afin de déplacer le contenu vers un pool de stockage sur bande.

Description de la tâche

Pour un serveur TSM, vous devez définir un pool de stockage sur bandes et un pool de stockage sur disque dans Tivoli Storage Manager. Une fois le pool de disques défini, créez un volume de disque et affectez-le au pool de disques. Un pool de bandes n'est pas nécessaire si votre serveur TSM utilise du stockage sur disque uniquement.

Vous devez effectuer plusieurs étapes sur votre serveur TSM avant de pouvoir créer un pool de stockage sur bandes. (Créez une bibliothèque de bandes et au moins un lecteur dans la bibliothèque de bandes. Définissez un chemin entre le serveur et la bibliothèque et entre le serveur et les lecteurs, puis définissez une classe de périphériques pour les lecteurs.) Les détails de ces étapes peuvent varier en fonction de la configuration matérielle et des besoins de stockage du site. Pour plus d'informations, consultez la documentation TSM.

Le jeu d'instructions ci-dessous illustre le processus. Vous devez savoir que les besoins spécifiques à votre site peuvent varier en fonction des besoins de votre déploiement. Pour plus d'informations sur la configuration

et pour obtenir des instructions, consultez la documentation TSM.



Vous devez vous connecter au serveur avec des privilèges d'administration et utiliser l'outil `dsmadm` pour exécuter les commandes suivantes.

Étapes

1. Créez une bibliothèque de bandes.

```
define library tapelibrary libtype=scsi
```

Où *tapelibrary* est un nom arbitraire choisi pour la bibliothèque de bandes et la valeur de *libtype* peut varier selon le type de bibliothèque de bandes.

2. Définissez un chemin entre le serveur et la bibliothèque de bandes.

```
define path servername tapelibrary srctype=server desttype=library device=lib-devicename
```

- ° *servername* Est le nom du serveur TSM
- ° *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini
- ° *lib-devicename* est le nom du périphérique de la bibliothèque de bandes

3. Définissez un lecteur pour la bibliothèque.

```
define drive tapelibrary drivename
```

- ° *drivename* est le nom que vous souhaitez spécifier pour le lecteur
- ° *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini

Il est possible que vous souhaitiez configurer un ou plusieurs lecteurs supplémentaires, en fonction de la configuration de votre matériel. (Par exemple, si le serveur TSM est connecté à un commutateur Fibre Channel qui comporte deux entrées d'une bibliothèque de bandes, vous pouvez définir un lecteur pour chaque entrée.)

4. Définissez un chemin entre le serveur et le lecteur que vous avez défini.

```
define path servername drivename srctype=server desttype=drive  
library=tapelibrary device=drive-dname
```

- ° *drive-dname* est le nom du périphérique du lecteur
- ° *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini

Répétez l'opération pour chaque lecteur que vous avez défini pour la bibliothèque de bandes à l'aide d'un lecteur distinct *drivename* et *drive-dname* pour chaque lecteur.

5. Définir une classe de périphérique pour les lecteurs.

```
define devclass DeviceClassName devtype=lto library=tapelibrary  
format=tapetype
```

- ° *DeviceClassName* est le nom de la classe de périphérique

- *lto* est le type de lecteur connecté au serveur
- *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini
- *tapetype* est le type de bande ; par exemple, *ultrium3*

6. Ajoutez des volumes de bande à l'inventaire de la bibliothèque.

```
checkin libvolume tapelibrary
```

tapelibrary est le nom de bibliothèque de bandes que vous avez défini.

7. Créez le pool de stockage sur bande primaire.

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxxscratch=XX
```

- *SGWSTapePool* Est le nom du pool de stockage de bandes du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage de bandes (tant que le nom utilise les conventions de syntaxe attendues par le serveur TSM).
- *DeviceClassName* est le nom de la classe de périphérique pour la bibliothèque de bandes.
- *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple : « pool de stockage sur bande pour le nœud d'archivage ».
- *collocate=filespace* Spécifie que le serveur TSM doit écrire des objets à partir du même espace de fichiers dans une seule bande.
- *xx* est l'une des suivantes :
 - Nombre de bandes vides dans la bibliothèque de bandes (dans le cas où le nœud d'archivage est la seule application utilisant la bibliothèque).
 - Nombre de bandes allouées pour l'utilisation par le système StorageGRID (dans les cas où la bibliothèque de bandes est partagée).

8. Sur un serveur TSM, créez un pool de stockage sur disque. Sur la console d'administration du serveur TSM, entrez

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* Est le nom du pool de disques du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage sur disque (tant que le nom utilise les conventions de syntaxe attendues par le TSM).
- *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple, "disque de stockage pool pour le nœud d'archivage".
- *maximum_file_size* force les objets de plus grande taille à être écrits directement sur bande, au lieu d'être mis en cache dans le pool de disques. Il est recommandé de le régler *maximum_file_size* À 10 Go.
- *nextstgpool=SGWSTapePool* Désigne le pool de stockage sur disque au pool de stockage sur bandes défini pour le nœud d'archivage.

- *percent_high* définit la valeur à laquelle le pool de disques commence à migrer son contenu vers le pool de bandes. Il est recommandé de le régler *percent_high* sur 0, pour que la migration des données commence immédiatement
- *percent_low* définit la valeur à laquelle la migration vers le pool de bandes s'arrête. Il est recommandé de le régler *percent_low* à 0 pour effacer le pool de disques.

9. Sur un serveur TSM, créez un ou plusieurs volumes de disque et affectez-les au pool de disques.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* est le nom du pool de disques.
- *volume_name* est le chemin complet vers l'emplacement du volume (par exemple, `/var/local/arc/stage6.dsm`) Sur le serveur TSM où il écrit le contenu du pool de disques en préparation du transfert sur bande.
- *size* Est la taille, en Mo, du volume de disque.

Par exemple, pour créer un volume de disque unique de sorte que le contenu d'un pool de disques remplisse une seule bande, définissez la valeur de la taille sur 200000 lorsque le volume de bande a une capacité de 200 Go.

Cependant, il est préférable de créer plusieurs volumes de disque de taille inférieure, car le serveur TSM peut écrire sur chaque volume du pool de disques. Par exemple, si la taille de la bande est de 250 Go, créez 25 volumes de disque d'une taille de 10 Go (10000) chacun.

Le serveur TSM préalloue de l'espace dans le répertoire du volume de disque. Cette opération peut prendre un certain temps (plus de trois heures pour un volume de disque de 200 Go).

Définissez une stratégie de domaine et enregistrez un nœud

Vous devez définir une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage, puis enregistrer un nœud pour utiliser cette stratégie de domaine.



Les processus du nœud d'archivage peuvent fuir de mémoire si le mot de passe client du nœud d'archivage dans Tivoli Storage Manager (TSM) expire. Assurez-vous que le serveur TSM est configuré de sorte que le nom d'utilisateur/mot de passe du client pour le nœud d'archivage n'expire jamais.

Lors de l'enregistrement d'un nœud sur le serveur TSM pour l'utilisation du nœud d'archivage (ou la mise à jour d'un nœud existant), vous devez spécifier le nombre de points de montage que le nœud peut utiliser pour les opérations d'écriture en spécifiant le paramètre MAXNUMMP à la commande ENREGISTRER NOEUD. Le nombre de points de montage est généralement équivalent au nombre de têtes de lecteur de bande attribuées au nœud d'archivage. Le numéro spécifié pour MAXNUMMP sur le serveur TSM doit être au moins aussi grand que la valeur définie pour **ARC Target Configuration main maximum Store sessions** pour le nœud d'archivage, Qui est défini sur 0 ou 1, car les sessions de stockage simultanées ne sont pas prises en charge par le nœud d'archivage.

La valeur MAXSESSIONS définie pour le serveur TSM contrôle le nombre maximal de sessions qui peuvent être ouvertes sur le serveur TSM par toutes les applications clientes. La valeur de MAXSESSIONS spécifiée sur le TSM doit être au moins aussi grande que la valeur spécifiée pour **ARC Target Configuration main nombre de sessions** dans le gestionnaire de grille pour le nœud d'archives. Le nœud d'archivage crée

simultanément au plus une session par point de montage et un petit nombre (5) de sessions supplémentaires.

Le nœud TSM affecté au nœud d'archivage utilise une stratégie de domaine personnalisée `tsm-domain`. Le `tsm-domain` La politique de domaine est une version modifiée de la politique de domaine « standard », configurée pour écrire sur bande et avec la destination d'archivage définie comme pool de stockage du système StorageGRID (`SGWSDiskPool`).



Vous devez vous connecter au serveur TSM avec des privilèges d'administration et utiliser l'outil `dsmadm` pour créer et activer la stratégie de domaine.

Créez et activez la stratégie de domaine

Vous devez créer une stratégie de domaine, puis l'activer pour configurer le serveur TSM afin d'enregistrer les données envoyées à partir du nœud d'archivage.

Étapes

1. Créer une stratégie de domaine.

```
copy domain standard tsm-domain
```

2. Si vous n'utilisez pas de classe de gestion existante, entrez l'une des options suivantes :

```
define policyset tsm-domain standard
```

```
define mgmtclass tsm-domain standard default
```

default est la classe de gestion par défaut pour le déploiement.

3. Créez un groupe de copie dans le pool de stockage approprié. Entrer (sur une ligne) :

```
define copygroup tsm-domain standard default type=archive  
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

default Est la classe de gestion par défaut du nœud d'archivage. Les valeurs de `retinit`, `retmin`, et `retver` Ont été choisis pour refléter le comportement de rétention actuellement utilisé par le nœud d'archivage



Ne pas régler `retinit` à `retinit=create`. Réglage `retinit=create` Bloque le nœud d'archivage de supprimer du contenu car les événements de rétention sont utilisés pour supprimer du contenu du serveur TSM.

4. Attribuez la classe de gestion à la valeur par défaut.

```
assign defmgmtclass tsm-domain standard default
```

5. Définissez la nouvelle règle sur active.

```
activate policyset tsm-domain standard
```

Ignorez l'avertissement « aucun groupe de copie de sauvegarde » qui s'affiche lorsque vous entrez la commande Activer.

6. Enregistrez un nœud pour utiliser le nouvel ensemble de règles sur le serveur TSM. Sur le serveur TSM, entrez (sur une ligne) :

```
register node arc-user arc-password passexp=0 domain=tsm-domain  
MAXNUMMP=number-of-sessions
```

Arc-user et arc-mot-de-passe sont les mêmes nom de nœud client et mot de passe que ceux définis sur le nœud d'archivage, et la valeur MAXNUMMP est définie sur le nombre de lecteurs de bande réservés pour les sessions de magasin de nœud d'archivage.



Par défaut, l'enregistrement d'un nœud crée un ID utilisateur administratif avec l'autorité propriétaire du client, avec le mot de passe défini pour le nœud.

Migrer les données vers StorageGRID

Vous pouvez migrer d'importants volumes de données vers le système StorageGRID tout en utilisant le système StorageGRID pour les opérations quotidiennes.

La section suivante est un guide pour comprendre et planifier la migration d'importants volumes de données vers le système StorageGRID. Ce n'est pas un guide général de la migration des données et n'inclut pas des étapes détaillées pour effectuer une migration. Suivez les instructions de cette section pour assurer une migration efficace des données dans le système StorageGRID sans perturber les opérations quotidiennes et que les données migrées sont correctement gérées par le système StorageGRID.

Vérifier la capacité du système StorageGRID

Avant de migrer d'importants volumes de données vers le système StorageGRID, vérifiez que le système StorageGRID dispose des capacités de disque nécessaires pour gérer le volume prévu.

Si le système StorageGRID inclut un nœud d'archivage et qu'une copie d'objets migrés a été enregistrée dans le stockage nearline (par exemple une bande), assurez-vous que la capacité de stockage du nœud d'archivage est suffisante pour le volume prévu de données migrées.

Dans le cadre de l'évaluation de la capacité, examinez le profil de données des objets que vous prévoyez de migrer et calculez la capacité de disque requise. Pour plus d'informations sur la surveillance de la capacité du disque de votre système StorageGRID, reportez-vous à la section [Gérer des nœuds de stockage](#) et [Surveiller et résoudre les problèmes](#).

Détermination de la règle ILM pour les données migrées

La règle ILM du système StorageGRID détermine le nombre de copies effectuées, l'emplacement des copies stockées et la durée de conservation de ces copies. Une règle ILM comprend un ensemble de règles ILM décrit la procédure de filtrage des objets et de gestion des données d'objet au fil du temps.

Selon l'utilisation des données migrées et vos exigences concernant les données migrées, vous pouvez définir des règles ILM uniques pour les données migrées qui ne sont pas les règles ILM utilisées pour les opérations quotidiennes. Par exemple, si la gestion quotidienne des données implique différentes exigences réglementaires que les données incluses dans la migration, il est possible de vouloir créer un nombre différent de copies des données migrées sur un niveau de stockage différent.

Vous pouvez configurer des règles qui s'appliquent exclusivement aux données migrées si une distinction unique entre les données migrées et les données objet enregistrées au quotidien.

Si vous faites la distinction de manière fiable entre les types de données en utilisant l'un des critères de métadonnées, ce critère vous permet de définir une règle ILM qui ne s'applique qu'aux données migrées.

Avant de commencer la migration des données, veillez à bien comprendre la règle ILM du système StorageGRID et la manière dont elle s'applique aux données migrées, et à effectuer et tester toutes les modifications apportées à la règle ILM. Voir [Gestion des objets avec ILM](#).



Une règle ILM incorrecte peut entraîner une perte de données irrécupérable. Examinez attentivement toutes les modifications apportées à une stratégie ILM avant de l'activer pour vous assurer que celle-ci fonctionne comme prévu.

Impact de la migration sur les opérations

Le système StorageGRID permet un fonctionnement efficace du stockage objet et de la récupération. Il offre une excellente protection contre la perte de données grâce à la création transparente de copies redondantes des données d'objet et des métadonnées.

Toutefois, la migration des données doit être gérée avec soin conformément aux instructions de ce chapitre pour éviter tout impact sur les opérations quotidiennes des systèmes ou, dans des cas extrêmes, placer les données en cas de perte en cas de défaillance du système StorageGRID.

La migration de volumes importants de données impose une charge supplémentaire au système. Lorsque le système StorageGRID est lourdement chargé, il répond plus lentement aux demandes de stockage et de récupération d'objets. Cela peut interférer avec les demandes de stockage et de récupération qui font partie intégrante des opérations quotidiennes. La migration peut également entraîner d'autres problèmes opérationnels. Par exemple, lorsqu'un nœud de stockage arrive à saturation de la capacité, la charge intermittente importante due à l'ingestion par lots peut faire basculer le nœud de stockage entre la lecture seule et la lecture-écriture, générant des notifications.

Si le chargement persiste, les files d'attente peuvent développer différentes opérations que le système StorageGRID doit exécuter pour assurer la redondance complète des données d'objet et des métadonnées.

La migration des données doit être gérée avec soin conformément aux directives présentées dans ce document afin de garantir un fonctionnement sûr et efficace du système StorageGRID pendant la migration. Lors de la migration des données, ingestion d'objets par lots ou ingestion continue. Ensuite, surveillez en continu le système StorageGRID pour vous assurer que les différentes valeurs d'attribut ne sont pas dépassées.

Planifiez et surveillez la migration des données

La migration des données doit être planifiée et contrôlée si nécessaire pour assurer le placement des données conformément à la politique ILM dans les délais impartis.

Planification de la migration des données

Évitez la migration des données pendant les heures de fonctionnement essentielles. Limitez la migration des données aux soirées, week-ends et autres fois que l'utilisation du système est faible.

Si possible, ne pas planifier de migration des données pendant les périodes d'activité élevée. Toutefois, s'il n'est pas pratique d'éviter complètement la période d'activité élevée, il est sûr de procéder aussi longtemps

que vous surveillez attentivement les attributs pertinents et que vous prenez des mesures s'ils dépassent les valeurs acceptables.

Surveiller la migration des données

Ce tableau répertorie les attributs que vous devez contrôler lors de la migration des données, ainsi que les problèmes qu'ils représentent.

Si vous utilisez des stratégies de classification du trafic avec des limites de taux pour accélérer l'entrée, vous pouvez surveiller le taux observé en conjonction avec les statistiques décrites dans le tableau suivant et réduire les limites si nécessaire.

Superviser	Description
Nombre d'objets en attente de l'évaluation ILM	1. Sélectionnez SUPPORT > Outils > topologie de grille. 2. Sélectionnez déploiement Présentation main. 3. Dans la section ILM Activity, surveillez le nombre d'objets affichés pour les attributs suivants : ◦ Attente - tous (XQUZ): Le nombre total d'objets en attente d'évaluation ILM. ◦ Attente - client (XCQZ) : nombre total d'objets en attente d'évaluation ILM des opérations client (par exemple, transfert). 4. Si le nombre d'objets affichés pour l'un de ces attributs dépasse 100,000, réduisez la vitesse d'entrée des objets afin de réduire la charge sur le système StorageGRID.
Capacité de stockage des systèmes d'archivage ciblés	Si la règle ILM enregistre une copie des données migrées vers un système de stockage d'archives ciblé (bande ou cloud), surveillez la capacité du système de stockage d'archivage ciblé pour s'assurer que la capacité disponible est suffisante.
Archive Node ARC Store	Si une alarme pour l'attribut Store Failures (ARVF) est déclenchée, le système de stockage d'archives ciblé a peut-être atteint sa capacité. Vérifiez le système de stockage d'archives ciblé et résolvez tout problème ayant déclenché une alarme.

Gestion des objets avec ILM

Gérez les objets avec ILM : présentation

Vous gérez les objets d'un système StorageGRID en configurant des règles et des règles de gestion du cycle de vie des informations (ILM). Grâce aux règles et règles ILM, StorageGRID explique comment créer et distribuer des copies de données d'objet, et comment gérer ces copies au fil du temps.

À propos de ces instructions

La conception et la mise en œuvre de règles ILM et de la politique ILM nécessitent une planification minutieuse. Vous devez connaître vos exigences opérationnelles, la topologie de votre système StorageGRID,

vos besoins en matière de protection des objets et les types de stockage disponibles. Ensuite, vous devez déterminer comment vous voulez que différents types d'objets soient copiés, distribués et stockés.

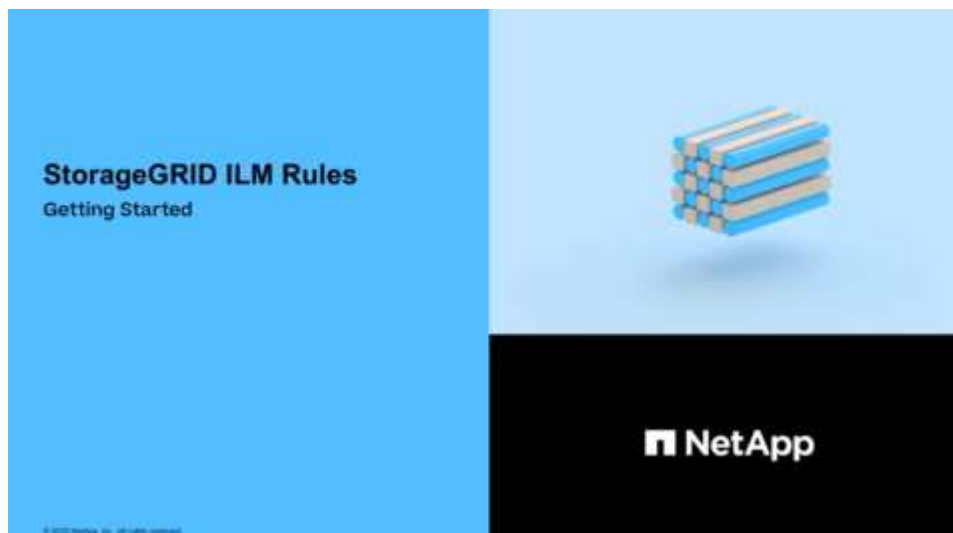
Suivez ces instructions pour :

- Découvrez la gestion du cycle de vie d'un objet StorageGRID, notamment son fonctionnement tout au long de sa durée de vie, ainsi que les règles et règles ILM.
- Découvrez comment configurer des pools de stockage, des profils de code d'effacement et des règles ILM.
- Découvrez comment créer et activer une règle ILM qui protège les données d'objet sur un ou plusieurs sites.
- Découvrez comment gérer les objets avec le verrouillage d'objet S3, qui vous permet de ne pas supprimer ou écraser les objets de certaines compartiments S3 pour une durée déterminée.

En savoir plus >>

Pour en savoir plus, consultez ces vidéos :

- ["Vidéo : règles ILM de StorageGRID : mise en route"](#)



- ["Vidéo : règles ILM de StorageGRID"](#)



ILM et cycle de vie des objets

Fonctionnement de ILM tout au long de la vie d'un objet

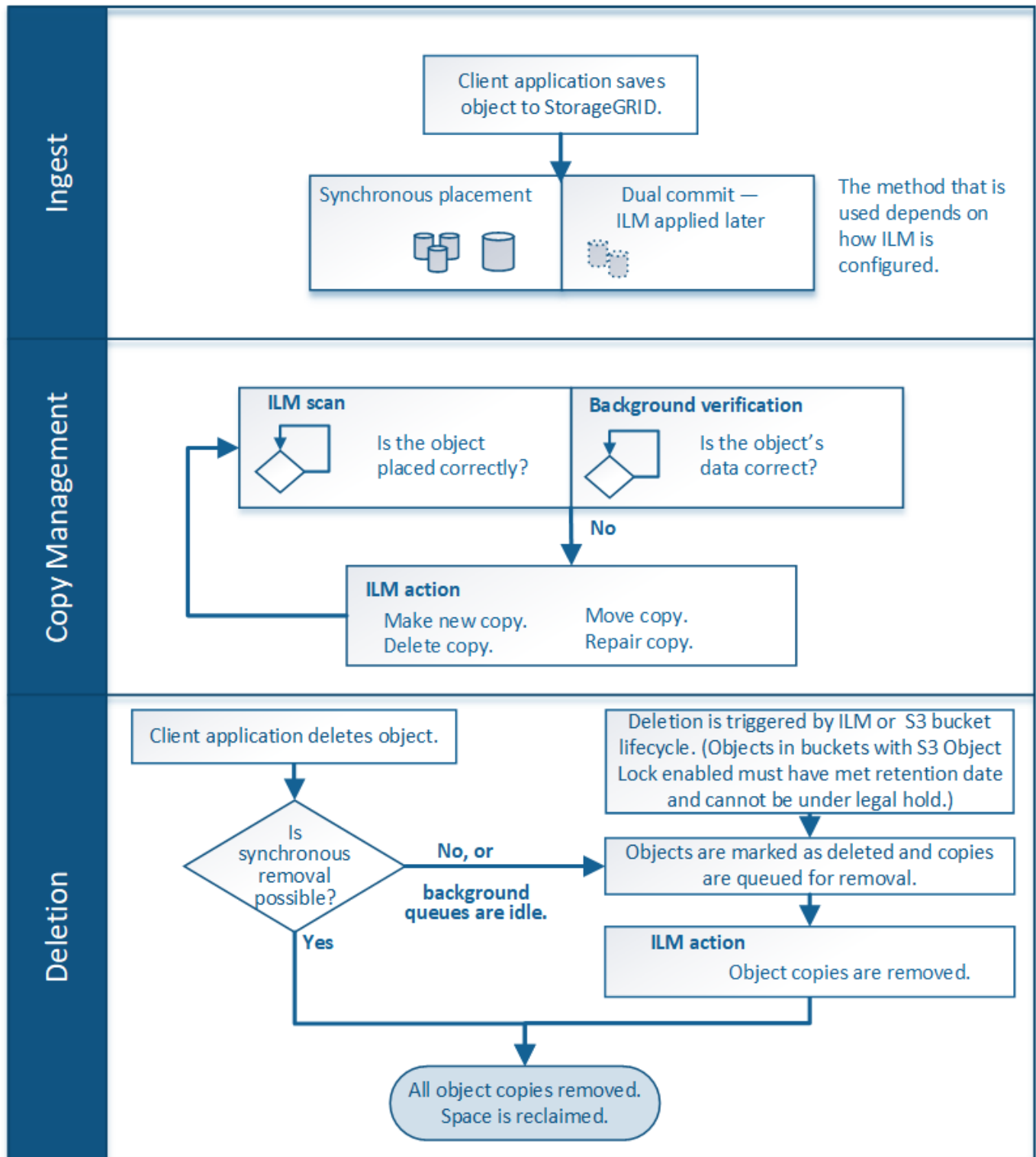
La compréhension de la façon dont StorageGRID utilise les règles ILM pour gérer les objets à chaque étape de leur vie peut vous aider à concevoir des règles plus efficaces.

- **InGest** : l'entrée commence lorsqu'une application client S3 ou Swift établit une connexion pour enregistrer un objet dans le système StorageGRID et est terminée lorsque StorageGRID renvoie un message « entrée réussie » au client. Les données d'objet sont protégées pendant l'ingestion, soit par application immédiate d'instructions ILM (placement synchrone), soit par création de copies intermédiaires et application de la règle ILM (double allocation), en fonction de la spécification des exigences ILM.
- **Gestion des copies** : après la création du nombre et du type de copies d'objets spécifiés dans les instructions de placement de l'ILM, StorageGRID gère les emplacements des objets et protège les objets contre les pertes.
 - Analyse et évaluation ILM : StorageGRID analyse en continu la liste des objets stockés dans la grille et vérifie si les copies actuelles répondent aux exigences ILM. Lorsque différents types, nombres ou emplacements de copies d'objets sont requis, StorageGRID crée, supprime ou déplace des copies selon les besoins.
 - Vérification en arrière-plan : StorageGRID effectue en permanence une vérification en arrière-plan afin de vérifier l'intégrité des données d'objet. En cas de problème, StorageGRID crée automatiquement une nouvelle copie objet ou un fragment d'objet de code d'effacement de remplacement à un emplacement conforme aux exigences ILM actuelles. Reportez-vous aux instructions pour [Contrôle et dépannage de StorageGRID](#).
- **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 dont le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont en attente légale ou si une date de conservation 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

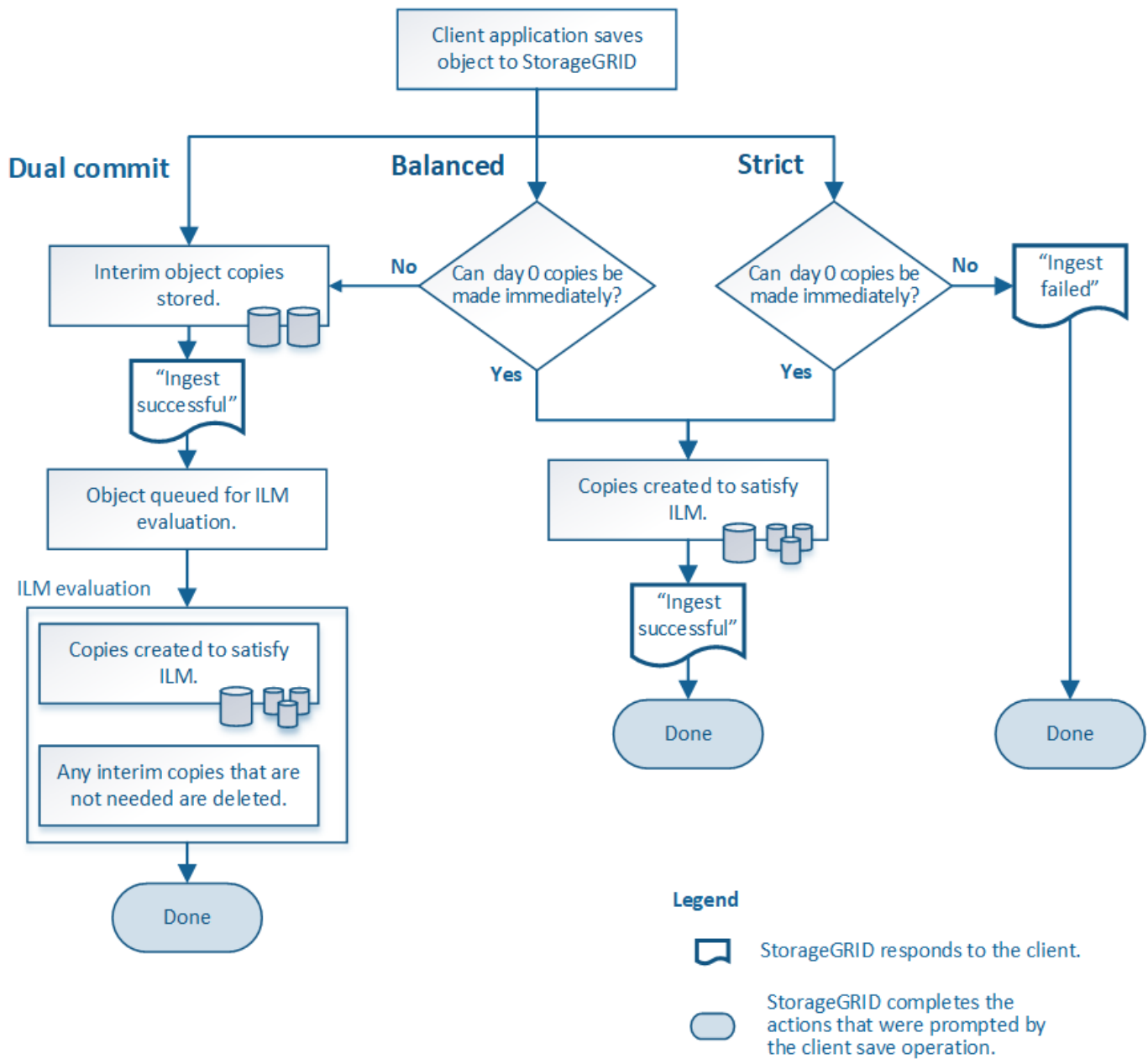
Options de protection des données pour l'ingestion

Lorsque vous créez une règle ILM, vous choisissez l'une des trois options de protection des objets à l'entrée : double allocation, équilibrage ou stricte. 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 trois options d'acquisition

L'organigramme indique ce qui se passe lorsque les objets sont mis en correspondance par une règle ILM qui utilise chacune des trois options d'ingestion.



Double allocation

Lorsque vous sélectionnez l'option Dual commit, StorageGRID effectue immédiatement des copies d'objet provisoires sur deux nœuds de stockage différents et renvoie un message « acquisition réussie » au client. L'objet est placé dans la file d'attente pour l'évaluation ILM et les copies correspondant aux instructions de placement de la règle sont créées ultérieurement.

Quand utiliser l'option Double validation

Utilisez l'option Dual commit dans l'un des cas suivants :

- Vous utilisez des règles ILM multisites et la latence d'ingestion du client est votre élément principal. Lorsque vous utilisez la double allocation, vous devez vous assurer que votre grid peut effectuer les tâches supplémentaires de création et de suppression des copies à double allocation s'il ne satisfait pas la solution ILM. Détails :
 - La charge sur la grille doit être suffisamment faible pour éviter un backlog ILM.
 - La grille doit disposer de ressources matérielles excessives (IOPS, processeur, mémoire, bande passante réseau, etc.).
- Vous utilisez des règles ILM multisites et la connexion WAN entre les sites présente généralement une latence élevée ou une bande passante limitée. Dans ce scénario, l'utilisation de l'option de double engagement permet d'éviter les délais d'attente du client. Avant de choisir l'option Dual commit, il est recommandé de tester l'application cliente avec des charges de travail réalistes.

Stricte

Lorsque vous sélectionnez une option stricte, StorageGRID utilise le placement synchrone pour l'ingestion et immédiatement toutes les copies d'objet spécifiées dans les instructions de placement de la règle. L'ingestion a échoué si StorageGRID ne peut pas créer toutes les copies, par exemple, car un emplacement de stockage requis est temporairement indisponible. Le client doit recommencer l'opération.

Quand utiliser l'option stricte

Utilisez l'option stricte si vous devez respecter des exigences opérationnelles ou réglementaires pour stocker immédiatement les objets aux emplacements définis dans la règle ILM. Par exemple, pour répondre à une exigence réglementaire, vous devez utiliser l'option stricte et un filtre avancé de contrainte d'emplacement pour garantir que les objets ne sont jamais stockés dans certains data centers.

Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict

Équilibré

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, StorageGRID ne peut pas faire immédiatement toutes les copies, utilise la fonction de double validation.

Quand utiliser l'option équilibrée

Utilisez l'option équilibrée afin de bénéficier de la meilleure combinaison possible de protection des données, de performances de grid et d'ingestion. Balance est l'option par défaut dans l'assistant de règles ILM.

Avantages, inconvénients et limites des options de protection des données

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.

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 équilibrée est recommandée sauf si un comportement d'entrée 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 et strictes, le message « acquisition réussie » n'est renvoyé au client que lorsque tous les fragments codés d'effacement ou copies répliquées sont créés et stockés. Néanmoins, les données d'objet atteindront leur placement final beaucoup plus vite.
- *** (Strict) taux d'échec d'entrée* plus élevés :** avec la stricte option, l'ingestion échoue lorsque StorageGRID ne peut pas immédiatement faire 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. Cependant, à l'aide d'un téléchargement partitionné et le ILM est évalué pour chaque partie de l'objet à son ingestion, et pour l'objet dans son ensemble une fois le téléchargement partitionné 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. À la place, toute pièce qui n'est pas correctement placée est mise en file d'attente pour la réévaluation de ILM et est déplacée ultérieurement vers le bon emplacement.
 - **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. Cela signifie que certaines parties d'un objet peuvent être stockées à des emplacements ne respectant pas les exigences ILM de l'objet dans son ensemble. 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'a pas été effectuée immédiatement. Les changements de placement sont apportés lorsqu'ILM est réévaluée par des processus ILM en arrière-plan normaux. Si les changements de positionnement requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement requis n'est pas disponible), l'objet mis à jour conserve son emplacement actuel jusqu'à ce que les changements de positionnement soient possibles.

Limites relatives au placement d'objets avec les options équilibrées ou strictes

Les options équilibrées ou strictes ne peuvent pas être utilisées pour les règles ILM dotées d'instructions de placement suivantes :

- Placement dans un pool de stockage cloud au premier jour.
- Placement dans un nœud d'archivage au jour 0.
- Parutions dans un pool de stockage cloud ou un nœud d'archivage 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 copie de manière synchrone sur un pool de stockage cloud ou un nœud d'archivage. En outre, un temps de création défini par l'utilisateur pourrait être résolu actuellement.

L'interaction des règles ILM et des contrôles de cohérence sur la protection des données

La règle ILM et le contrôle de cohérence de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le comportement d'ingestion sélectionné dans une règle ILM affecte le placement initial des copies d'objet, tandis que le contrôle de cohérence utilisé lors du stockage d'un objet affecte le placement initial des métadonnées d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Voici un résumé des contrôles de cohérence disponibles dans StorageGRID :

- **Tous** : tous les nœuds reçoivent immédiatement des métadonnées d'objet ou la demande échouera.
- **Strong-global**: Les métadonnées d'objet sont immédiatement distribuées à tous les sites. Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Site fort**: Les métadonnées d'objet sont immédiatement distribuées aux autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
- **Lecture-après-nouvelle-écriture** : offre une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties.
- **Disponible** (cohérence éventuelle pour les opérations DE TÊTE) : se comporte de la même façon que le niveau de cohérence "entre les nouvelles écritures", mais ne fournit qu'une cohérence éventuelle pour les opérations DE TÊTE.



Avant de sélectionner un niveau de cohérence, lisez la description complète des contrôles de cohérence dans les instructions pour [S3](#) ou [SWIFT](#) applications client. Vous devez comprendre les avantages et les limites avant de modifier la valeur par défaut.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. L'objet ne peut pas être récupéré.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

- [Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict](#)

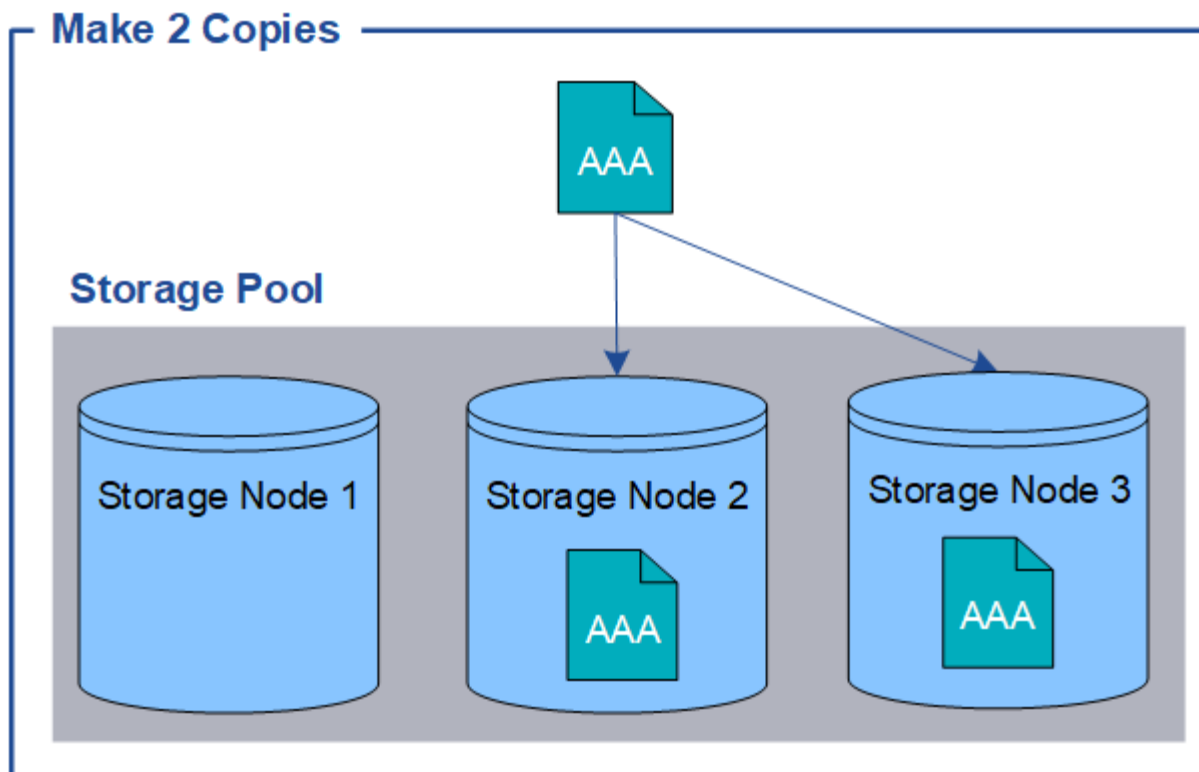
Le mode de stockage des objets (réplication ou code d'effacement)

Qu'est-ce que la réplication

La réplication est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objet. Lorsque les objets correspondent à une règle ILM utilisant la réplication, le système crée des copies exactes des données d'objet et stocke les copies sur les nœuds de stockage ou les nœuds d'archivage.

Lorsque vous configurez une règle ILM pour créer des copies répliquées, vous spécifiez le nombre de copies à créer, l'emplacement où elles doivent être stockées, ainsi que la durée de stockage de ces copies à chaque emplacement.

L'exemple de règle ILM décrit deux copies répliquées de chaque objet placées dans un pool de stockage contenant trois nœuds de stockage.



Lorsque StorageGRID met les objets en correspondance avec cette règle, elle crée deux copies de l'objet, en plaçant chaque copie sur un autre nœud de stockage du pool. Les deux copies peuvent être placées sur deux des trois nœuds de stockage disponibles. Dans ce cas, la règle a placé des copies d'objet sur les nœuds de stockage 2 et 3. Comme il existe deux copies, l'objet peut être récupéré en cas de défaillance de l'un des nœuds du pool de stockage.



StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si le grid inclut trois nœuds de stockage et que vous créez une règle ILM de 4 copies, seules trois copies sont effectuées, une copie pour chaque nœud de stockage. L'alerte **ILM placement inaccessible** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Informations associées

- [Qu'est-ce qu'un pool de stockage](#)
- [Utilisation de plusieurs pools de stockage pour la réplication intersites](#)

Pourquoi ne pas utiliser la réplication à copie unique

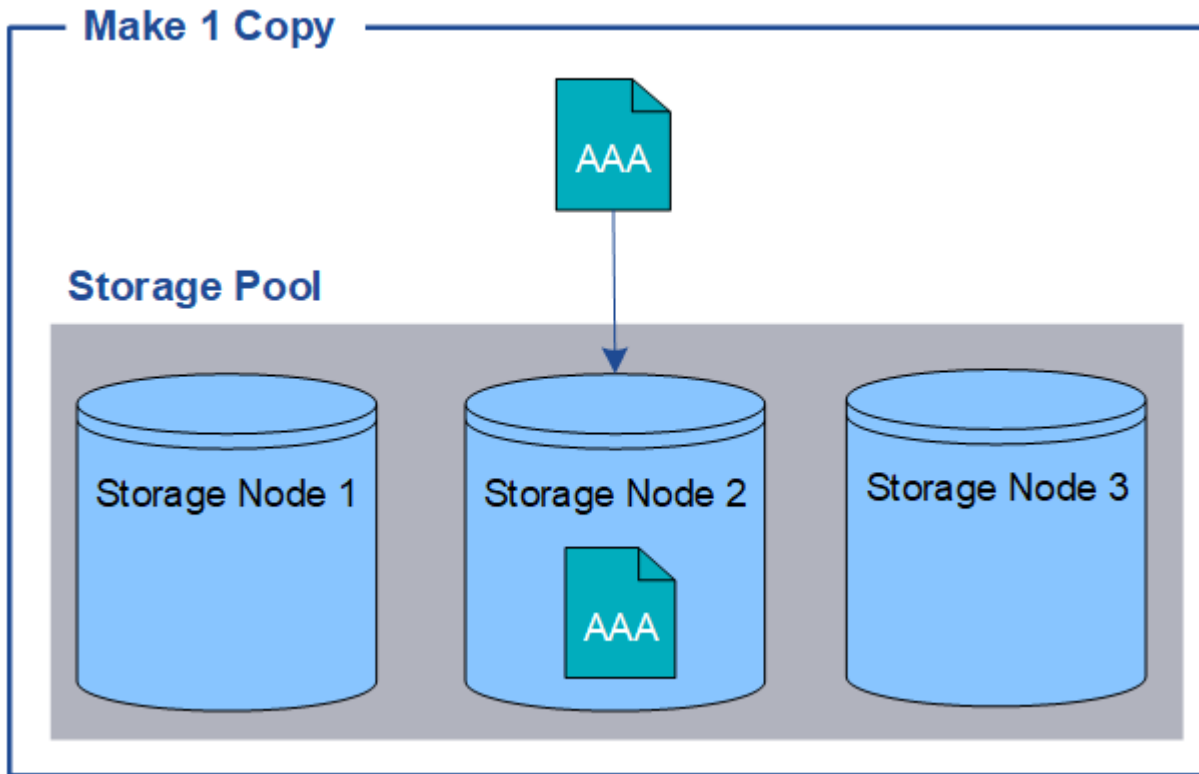
Lors de la création d'une règle ILM pour créer des copies répliquées, vous devez toujours spécifier au moins deux copies pour une période donnée dans les instructions de placement.



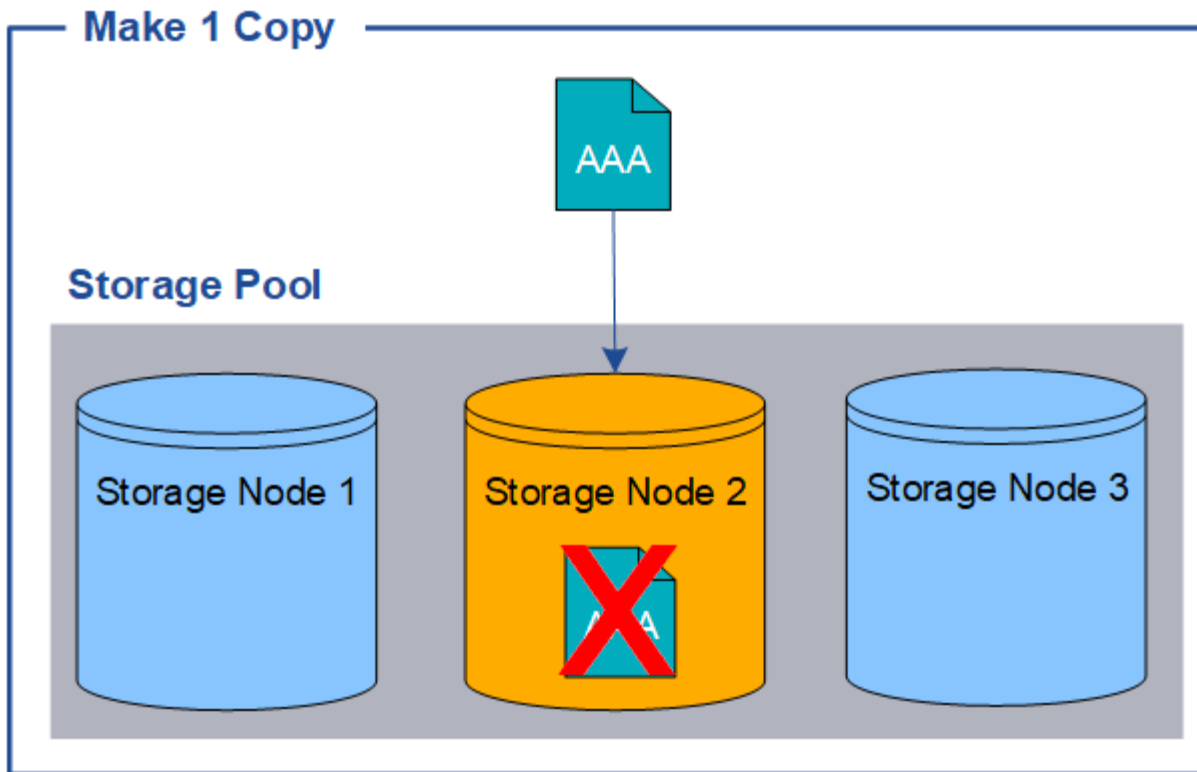
N'utilisez pas de règle ILM pour créer une seule copie répliquée pendant une période donnée. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un nœud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, 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.

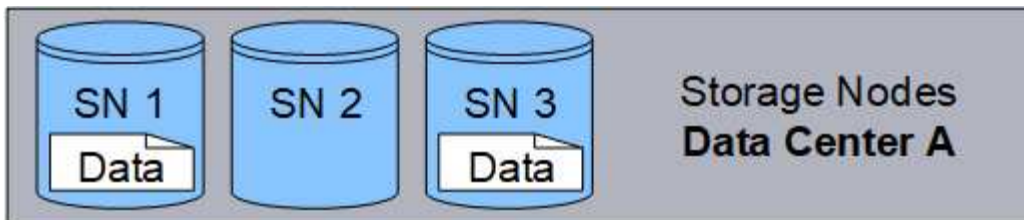


Pour éviter de perdre des données d'objet, vous devez toujours effectuer au moins deux copies de tous les objets à protéger par la réplication. Si deux copies ou plus existent, vous pouvez toujours accéder à l'objet en cas de panne ou de mise hors ligne d'un nœud de stockage.

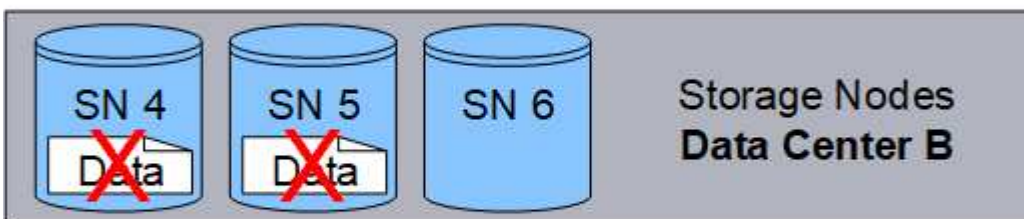
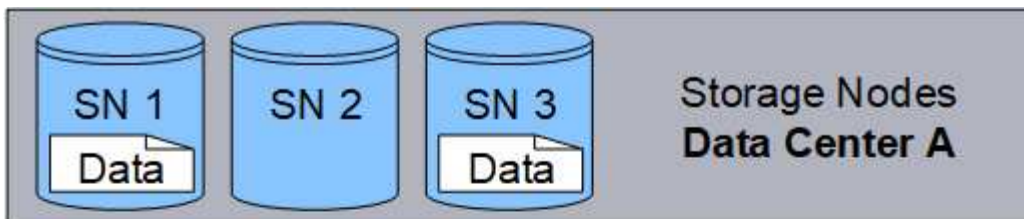
Qu'est-ce que le code d'effacement

Le codage d'effacement est la deuxième méthode utilisée par StorageGRID pour stocker les données d'objet. 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 code d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des données restantes et des fragments de parité.

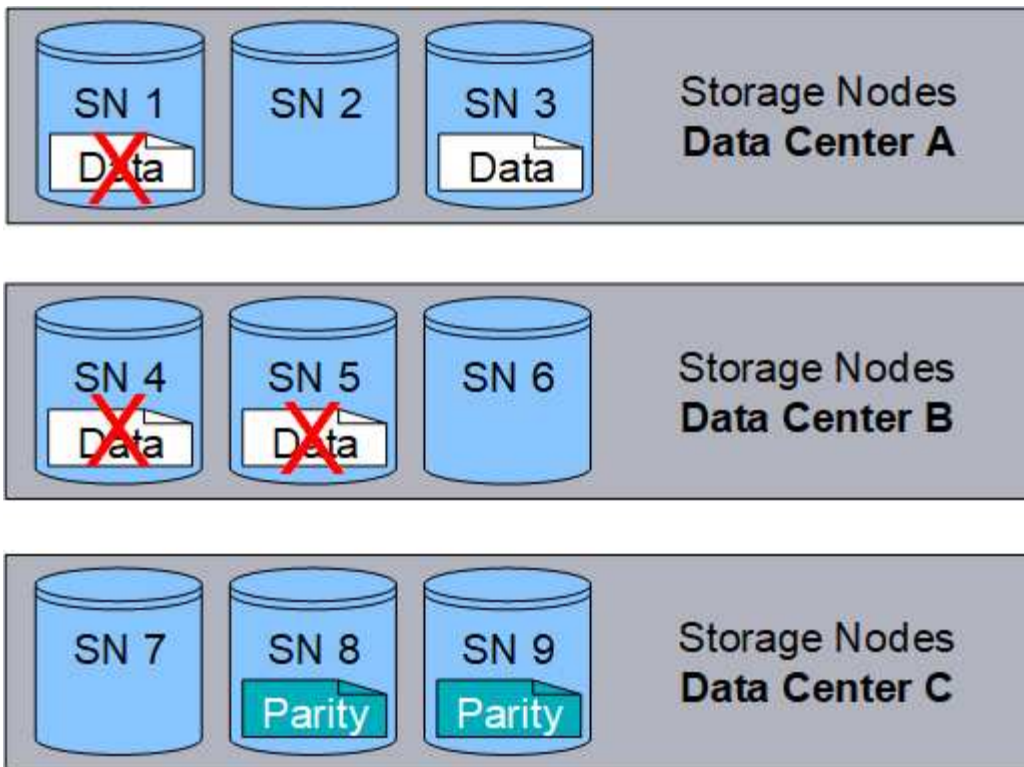
L'exemple suivant illustre l'utilisation d'un algorithme de code d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de code d'effacement 4+2. Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données 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 des 4+2 requiert au moins neuf nœuds de stockage, avec trois nœuds de stockage sur chacun de trois sites différents. 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. En cas de perte d'un site de data Center complet, 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 qu'un pool de stockage](#)
- [En quoi consiste les schémas de code d'effacement](#)
- [Créez un profil de code d'effacement](#)

En quoi consiste les schémas de code d'effacement

Lorsque vous configurez le profil de code d'effacement pour une règle ILM, vous sélectionnez un schéma de code d'effacement disponible en fonction du nombre de nœuds et de sites de stockage que vous prévoyez d'utiliser. Les schémas de codage d'effacement contrôlent le nombre de fragments de données et le nombre de fragments de parité créés pour chaque objet.

Le système StorageGRID utilise l'algorithme de codage d'effacement Reed-Solomon. L'algorithme coupe un objet en k fragments de données et calcule des fragments de parité M . Les fragments $k + m = n$ sont répartis sur n nœuds de stockage pour assurer la protection des données. Un objet peut supporter jusqu'à m fragments perdus ou corrompus. k fragments sont nécessaires pour récupérer ou réparer un objet.

Lors de la configuration d'un profil de code d'effacement, utilisez les règles suivantes pour les pools de stockage :

- Le pool de stockage doit inclure trois sites ou plus, ou exactement un site.



Vous ne pouvez pas configurer un profil de code d'effacement 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 le pool de stockage par défaut, tous les nœuds de stockage ou un pool de stockage incluant le site par défaut, tous les sites.
- Le pool de stockage doit inclure au moins $k+m+1$ nœuds de stockage.

Le nombre minimum 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.

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 avec la valeur totale la plus basse de $k+m$ qui répond à vos besoins. Les schémas de code d'effacement avec un nombre inférieur de fragments sont globalement plus efficaces du point de vue de la capacité de calcul, car moins de fragments sont créés et distribués (ou récupérés) par objet. Cela permet d'obtenir de meilleures performances en raison de la taille de fragment plus grande, et peut nécessiter moins de nœuds lors d'une extension lorsque plus de stockage est nécessaire. (Pour plus d'informations sur la planification d'une extension du stockage, consultez les instructions relatives à l'extension d'StorageGRID.)

Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites

Le tableau ci-dessous décrit les schémas de code d'effacement actuellement pris en charge par StorageGRID pour les pools de stockage incluant au moins trois sites. Tous ces plans offrent une protection contre la perte du site. Un site peut être perdu et l'objet sera toujours accessible.

Pour les schémas de code d'effacement qui assurent la 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 %

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
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 d'échecs, en utilisant un schéma avec plus de fragments (c'est-à-dire un total plus élevé pour $k+m$) crée plus de trafic réseau.
- **Surcharge de stockage :** les schémas qui génèrent une surcharge plus élevée requièrent davantage d'espace de stockage par objet.

Par exemple, lorsque vous décidez d'un schéma 4+2 et 6+3 (qui ont tous deux des frais de stockage de 50 %), sélectionnez le schéma 6+3 si une tolérance de panne supplémentaire est nécessaire. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées. Si tous les autres facteurs sont égaux, sélectionnez 4+2 parce qu'il a un nombre total de fragments inférieur.



Si vous n'êtes pas certain du schéma à utiliser, sélectionnez 4+2 ou 6+3, ou contactez le support technique.

Schémas de code d'effacement pour pools de stockage sur un site

Un pool de stockage sur un site prend en charge tous les schémas de codage d'effacement définis pour trois sites ou plus, à condition que le site dispose de suffisamment de nœuds de stockage.

Le nombre minimum de nœuds de stockage requis est $k+m$, mais un pool de stockage avec $k+m+1$ 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 %

Informations associées

[Développez votre grille](#)

Avantages, inconvénients et exigences du code d'effacement

Avant de décider s'il est nécessaire d'utiliser la réplication ou le codage d'effacement pour protéger les données d'objet contre la perte, vous devez connaître les avantages, les inconvénients et les exigences du codage d'effacement.

Avantages du code d'effacement

Par rapport à la réplication, le codage d'effacement assure une fiabilité, une disponibilité et une efficacité du stockage supérieures.

- **Fiabilité** : La fiabilité est évaluée en termes de tolérance de pannes, c'est-à-dire le nombre de défaillances simultanées qui peuvent être soutenues sans perte de données. Avec la réplication, plusieurs copies identiques sont stockées sur différents nœuds et entre plusieurs sites. Avec le codage d'effacement, un objet est codé en données et fragments de parité, puis distribué sur de nombreux nœuds et sites. Cette dispersion assure à la fois la protection des pannes sur le site et sur les nœuds. Par rapport à la réplication, le codage d'effacement améliore la fiabilité pour des coûts de stockage comparables.
- **Disponibilité** : la disponibilité peut être définie comme la possibilité de récupérer des objets en cas de défaillance ou d'accès aux nœuds de stockage. Par rapport à la réplication, le codage d'effacement assure une disponibilité supérieure et un coût de stockage comparable.
- **Efficacité du stockage** : pour des niveaux similaires de disponibilité et de fiabilité, les objets protégés par le codage d'effacement consomment moins d'espace disque que les mêmes objets s'ils sont protégés par la réplication. Par exemple, un objet de 10 Mo répliqué sur deux sites consomme 20 Mo d'espace disque (deux copies), tandis qu'un objet dont le code d'effacement est appliqué à trois sites et dont le schéma de code d'effacement 6+3 n'utilise que 15 Mo d'espace disque.



L'espace disque des objets avec code d'effacement est calculé selon la taille de l'objet et la surcharge du stockage. Le pourcentage de surcharge de stockage est le nombre de fragments de parité divisé par le nombre de fragments de données.

Inconvénients du code d'effacement

Par rapport à la réplication, le code d'effacement présente les inconvénients suivants :

- Cela nécessite un nombre accru de nœuds et de sites de stockage. Par exemple, si vous utilisez un schéma de code d'effacement de 6+3, vous devez disposer d'au moins trois nœuds de stockage sur trois sites différents. Au contraire, si vous répliquez simplement les données d'objet, vous ne avez besoin que d'un seul nœud de stockage pour chaque copie.
- Coût et complexité accrus de l'expansion du stockage. Pour étendre un déploiement qui utilise la réplication, il vous suffit d'ajouter 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 de 100 %, vous devez ajouter au moins $k+m$ nœuds de stockage. Cependant, si vous augmentez la capacité des nœuds existants à 70 %, vous pouvez ajouter deux nœuds par site tout en optimisant la capacité de stockage utilisable. Pour plus d'informations, voir [Ajoutez de la capacité de stockage pour les objets avec code d'effacement](#).
- Le codage d'effacement entre sites répartis géographiquement augmente la latence de récupération. Les fragments d'objet d'un objet dont le code d'effacement est codé et distribué sur des sites distants sont plus longs à extraire les connexions WAN que les objets répliqués et disponibles localement (sur le même site que celui sur lequel le client se connecte).
- Lorsque vous utilisez le codage d'effacement sur des sites répartis géographiquement, le trafic réseau WAN est plus important pour les récupérations et les réparations, en particulier pour les objets fréquemment récupérés ou pour la réparation d'objets via les connexions réseau WAN.
- Lorsque vous utilisez le codage d'effacement sur plusieurs sites, le débit maximal d'objets diminue considérablement à mesure que la latence du réseau entre les sites augmente. Cette diminution est due à la diminution correspondante du débit du réseau TCP, ce qui affecte la rapidité avec laquelle le système StorageGRID peut stocker et récupérer des fragments d'objet.
- Plus grande utilisation des ressources de calcul.

Quand utiliser le code d'effacement

Le code d'effacement convient mieux aux exigences suivantes :

- Objets dont la taille est supérieure à 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement.

- Stockage à long terme ou à froid pour le contenu rarement récupéré.
- Haute disponibilité et fiabilité des données.
- Protégez-vous contre les défaillances complètes du site et des nœuds.
- Efficacité du stockage.

- Les déploiements sur un seul site exigent une protection efficace des données avec une seule copie avec code d'effacement plutôt que plusieurs copies répliquées.
- Déploiements sur plusieurs sites pour lesquels la latence inter-site est inférieure à 100 ms.

Méthode de détermination de la conservation des objets

StorageGRID fournit aux administrateurs du grid et aux utilisateurs de locataires individuels les options permettant de spécifier la durée de stockage des objets. En général, les instructions de conservation fournies par un utilisateur locataire ont priorité sur les instructions de conservation fournies par l'administrateur de la grille.

Contrôle de la conservation des objets par les utilisateurs locataires

Les locataires disposent de trois méthodes principales pour contrôler la durée de stockage de leurs objets dans StorageGRID :

- Si le paramètre global S3 Object Lock est activé pour la grille, les locataires S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation à la date et la conservation légale de chaque version d'objet ajoutée dans ce compartiment.
 - Une version d'objet qui est en attente légale ne peut être supprimée par aucune méthode.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut pas être supprimée par aucune méthode.
 - Les objets des compartiments où le verrouillage d'objet S3 est activé sont conservés par ILM « Forever ». Une fois la date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou l'expiration du cycle de vie du compartiment. Voir [Gestion des objets avec le verrouillage d'objets S3](#).
- Les locataires S3 peuvent ajouter une configuration du cycle de vie à leurs compartiments pour définir une action d'expiration. En cas de cycle de vie d'un compartiment, StorageGRID stocke un objet jusqu'à ce que la date ou le nombre de jours spécifiés dans l'action expiration soit atteint, à moins que le client ne supprime d'abord l'objet. Voir [Création de la configuration du cycle de vie S3](#).
- Un client S3 ou Swift peut émettre une demande de suppression d'objet. StorageGRID privilégie toujours les demandes de suppression client sur le cycle de vie du compartiment S3 ou la ILM pour déterminer si supprimer ou conserver un objet.

Comment les administrateurs du grid contrôlent-ils la conservation des objets

Les administrateurs du grid utilisent des instructions de placement ILM pour contrôler la durée de stockage des objets. Lorsque les objets sont comparés par une règle ILM, StorageGRID les stocke jusqu'à la dernière période de la règle ILM. Les objets sont conservés indéfiniment si « toujours » est spécifié pour les instructions de placement.

Quelle que soit la durée de conservation des objets, les paramètres ILM contrôlent les types de copies d'objet (répliquées ou avec code d'effacement) stockés et l'emplacement des copies (nœuds de stockage, pools de stockage cloud ou nœuds d'archivage).

Interaction du cycle de vie des compartiments S3 et de la ILM

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

Exemples de conservation d'objets

Pour mieux comprendre les interactions entre le verrouillage objet S3, les paramètres du cycle de vie des compartiments, les demandes de suppression de clients et la gestion des règles ILM, prenez en compte ces exemples.

Exemple 1 : le cycle de vie des compartiments S3 permet de conserver les objets plus longtemps que ILM

ILM

Stockez deux copies pendant 1 an (365 jours)

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Résultat

StorageGRID stocke l'objet pendant 730 jours. StorageGRID utilise les paramètres du cycle de vie du compartiment pour déterminer s'il faut supprimer ou conserver un objet.



Si le cycle de vie des compartiments précise que les objets doivent être conservés plus longtemps que spécifié par l'ILM, StorageGRID continue d'utiliser les instructions de placement du ILM pour déterminer le nombre et le type de copies à stocker. Dans cet exemple, deux copies de l'objet continueront à être stockées dans StorageGRID au lieu de 366 à 730 jours.

Exemple 2 : le cycle de vie des compartiments S3 expire les objets avant la gestion du cycle de vie des règles

ILM

Stockage de deux copies pendant 2 ans (730 jours)

Cycle de vie des compartiments

Expiration des objets en 1 an (365 jours)

Résultat

StorageGRID supprime les deux copies de l'objet après le jour 365.

Exemple 3 : la suppression du client annule le cycle de vie du compartiment et la ILM

ILM

Stockage de deux copies sur des nœuds de stockage « toujours »

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Demande de suppression du client

Émis le jour 400

Résultat

StorageGRID supprime les deux copies de l'objet le jour 400 en réponse à la requête de suppression du client.

Exemple 4 : le verrouillage d'objet S3 remplace la demande de suppression du client

Verrouillage d'objet S3

Conserver jusqu'à ce jour pour une version d'objet : 2026-03-31. Une obligation légale n'est pas en vigueur.

Règle ILM conforme

Stockez deux copies sur des nœuds de stockage « toujours ».

Demande de suppression du client

Émis le 2024-03-31.

Résultat

StorageGRID ne supprimera pas la version de l'objet car la date de conservation est encore à 2 ans.

Comment supprimer les objets

StorageGRID peut supprimer des objets en réponse directe à une requête d'un client ou automatiquement à la suite de l'expiration du cycle de vie d'un compartiment S3 ou des exigences de la politique ILM. Pour gérer plus efficacement les objets, il est important de comprendre les différentes méthodes de suppression des objets et la façon dont StorageGRID les gère.

StorageGRID peut utiliser l'une des deux méthodes suivantes pour supprimer les objets :

- Suppression synchrone : lorsque StorageGRID reçoit une demande de suppression de client, toutes les copies d'objet sont supprimées immédiatement. Le client est informé que la suppression a réussi une fois les copies supprimées.
- Les objets sont placés en file d'attente pour suppression : lorsque StorageGRID reçoit une requête de suppression, l'objet est mis en attente pour suppression et le client est immédiatement informé de l'réussie de cette suppression. Les copies d'objet sont supprimées ultérieurement par le traitement ILM en arrière-plan.

Lors de la suppression d'objets, StorageGRID utilise la méthode qui optimise les performances de suppression, réduit les retards de suppression et libère de l'espace le plus rapidement possible.

Le tableau résume le moment où StorageGRID utilise chaque méthode.

Méthode d'exécution de la suppression	Lorsqu'il est utilisé
Les objets sont placés en file d'attente pour suppression	Lorsque l'une des conditions suivantes est vraie : - La suppression automatique d'objet a été déclenchée par l'un des événements suivants : - La date d'expiration ou le nombre de jours pendant la configuration du cycle de vie d'un compartiment S3 est atteint. - La dernière période spécifiée dans une règle ILM s'écoule. Remarque : les objets d'un compartiment dont le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont en attente légale ou si une date de conservation a été spécifiée mais pas encore remplie. - Un client S3 ou Swift demande la suppression d'une ou plusieurs des conditions suivantes : - Les copies ne peuvent pas être supprimées dans les 30 secondes, car un emplacement d'objet est temporairement indisponible, par exemple. - Les files d'attente de suppression d'arrière-plan sont inactives.
Suppression immédiate d'objets (suppression synchrone)	Lorsqu'un client S3 ou Swift effectue une demande de suppression et toutes des conditions suivantes sont remplies : - Toutes les copies peuvent être supprimées en 30 secondes. - Les files d'attente de suppression d'arrière-plan contiennent des objets à traiter.

Lorsque les clients S3 ou Swift font des demandes de suppression, StorageGRID commence par ajouter un certain nombre d'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.

Délai de suppression des objets

La façon dont StorageGRID supprime des objets peut avoir un impact sur le fonctionnement du système :

- Lorsque StorageGRID effectue une suppression synchrone, StorageGRID peut donner jusqu'à 30 secondes pour renvoyer un résultat au client. Cela signifie que la suppression peut se produire plus lentement, même si les copies sont réellement supprimées plus rapidement que lors de la mise en file d'attente d'objets StorageGRID pour suppression.
- Si vous surveillez de près les performances de suppression lors d'une suppression en bloc, vous remarquerez que ce taux de suppression semble ralentir après la suppression d'un certain nombre d'objets. Ce changement survient lorsque StorageGRID passe d'objets de mise en file d'attente pour suppression à des fins de suppression synchrone. La réduction apparente du taux de suppression ne signifie pas que les copies d'objet sont supprimées plus lentement. Au contraire, elle indique qu'en moyenne, l'espace est maintenant libéré plus rapidement.

Si vous supprimez un grand nombre d'objets et que vous souhaitez libérer rapidement de l'espace, pensez à utiliser une requête client pour supprimer des objets au lieu de les supprimer à l'aide d'ILM ou d'autres méthodes. En général, l'espace est libéré plus rapidement lors de la suppression d'espace par les clients, car StorageGRID peut utiliser la suppression synchrone.

Notez que 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'objet ne suppriment pas la version actuelle de l'objet et ne libère pas d'espace. Au lieu de cela, une requête de suppression d'objet crée simplement un marqueur de suppression comme version actuelle de l'objet, ce qui fait de la version précédente de l'objet « non courant ».

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.

Pour libérer de l'espace lors de la suppression d'objets multiversion, vous devez effectuer l'une des opérations suivantes :

- **Demande client S3** : spécifiez le numéro de version de l'objet dans la demande de SUPPRESSION d'objet S3 (`DELETE /object?versionId=ID`). Notez que cette demande ne supprime que les copies d'objet pour la version spécifiée (les autres versions occupent toujours de l'espace).
- **Cycle de vie du godet** : utilisez le `NoncurrentVersionExpiration` l'action en termes de configuration du cycle de vie des compartiments. Lorsque le nombre de `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.
- **ILM** : ajoutez deux règles ILM à votre politique ILM. Utilisez **Noncurrent Time** comme temps de référence dans la première règle pour correspondre aux versions non courantes de l'objet. Utilisez **temps d'ingestion** dans la deuxième règle pour correspondre à la version actuelle. La règle **Noncurrent Time** doit figurer dans la stratégie au-dessus de la règle **Ingest Time**.

Informations associées

- [Utilisation de S3](#)
- [Exemple 4 : règles et règles ILM pour les objets avec version S3](#)

Définition d'une règle ILM

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.

Comment une règle ILM évalue-t-elle les objets ?

La règle ILM active pour votre système StorageGRID permet de contrôler le placement, la durée et la protection des données de tous les objets.

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

1. Si les filtres de la première règle de la règle correspondent à un objet, celui-ci est ingéré conformément au comportement d'ingestion de cette règle et stocké conformément aux instructions de placement de cette règle.
2. Si les filtres de la première règle ne correspondent pas à l'objet, celui-ci est évalué par rapport à chaque règle ultérieure de la stratégie jusqu'à ce qu'une correspondance soit effectuée.
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, tous les compartiments et toutes les versions d'objet et ne peut pas utiliser de filtres avancés.

Exemple de règle ILM

Cet exemple de politique ILM utilise trois règles ILM.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Example ILM policy

Reason for change

New policy

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

	Default	Rule Name	Tenant Account	Actions
+		Rule 1: 3 replicated copies for Tenant A	Tenant A (58889986524346589742)	×
+		Rule 2: Erasure coding for objects greater than 1 MB	—	×
	✓	Rule 3: 2 copies 2 data centers (default)	—	×

Cancel

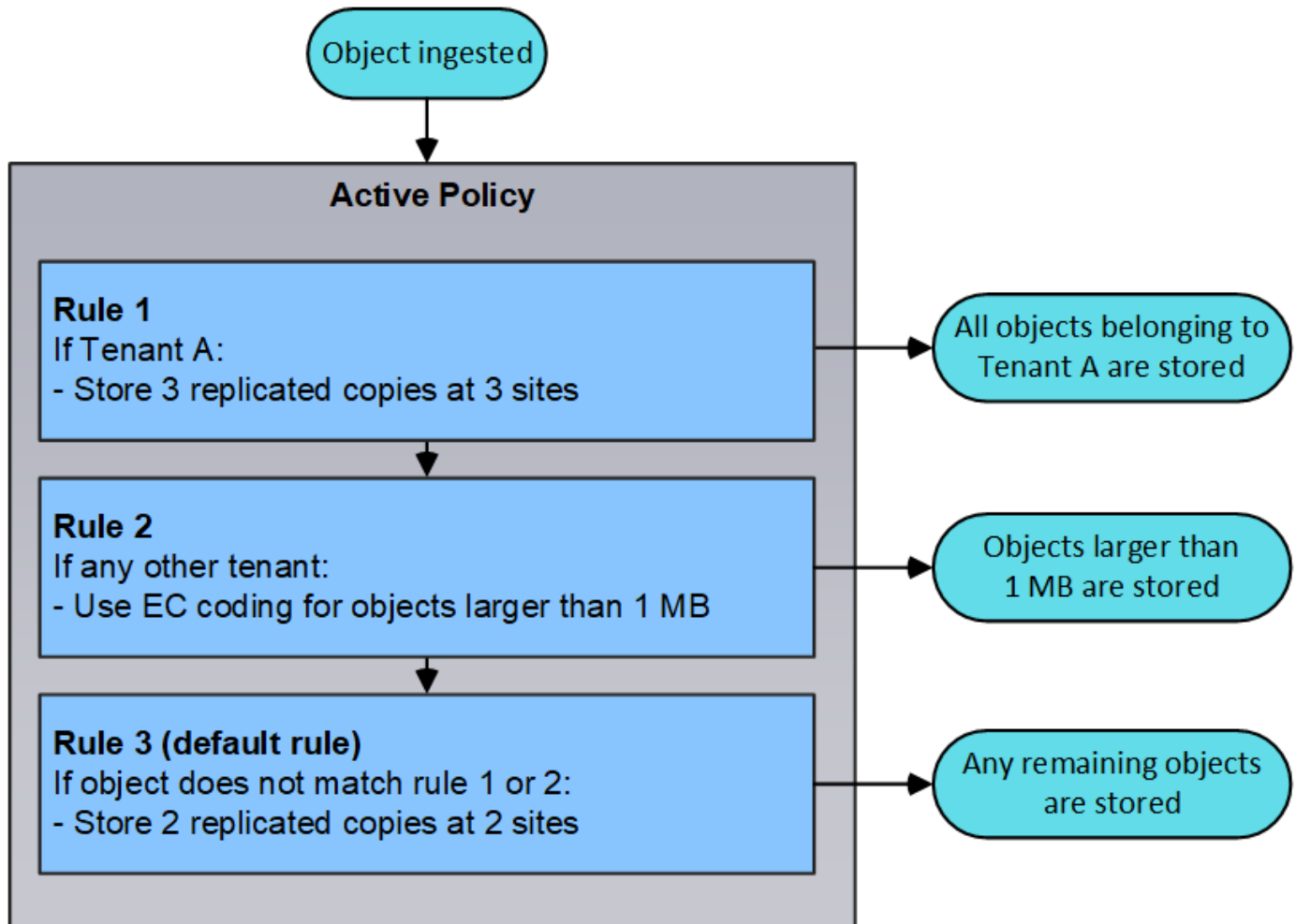
Save

Dans cet exemple, la règle 1 correspond à tous les objets appartenant au locataire A. Ces objets sont stockés sous forme de trois copies répliquées sur trois sites. Les objets appartenant à d'autres locataires ne sont pas mis en correspondance par la règle 1, ils sont donc évalués par rapport à la règle 2.

La règle 2 correspond à 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. La règle 2 ne correspond pas aux objets de 1 Mo ou plus petits, de sorte que ces objets sont évalués par rapport à la règle 3.

La règle 3 est la dernière et la règle par défaut de la stratégie, et elle n'utilise pas de filtres. La règle 3 effectue deux copies répliquées de tous les objets qui ne correspondent pas à la règle 1 ou à la règle 2 (les objets n'appartenant pas au locataire A dont la taille est inférieure ou égale à 1 Mo).



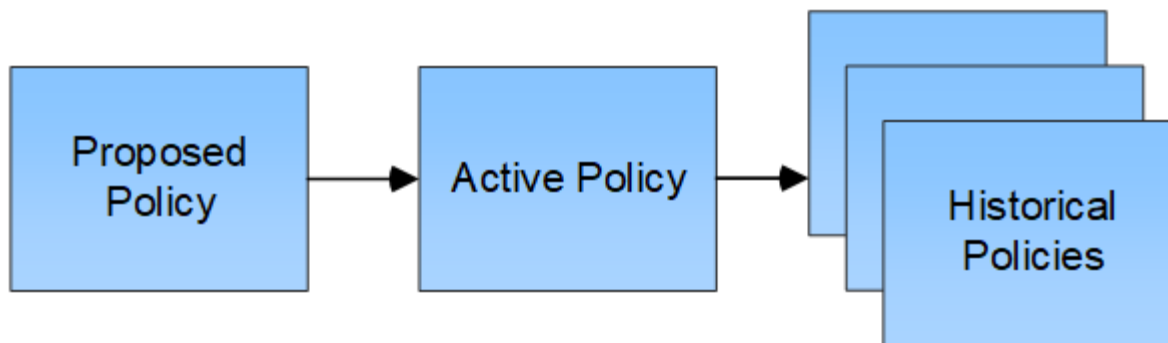
Quelles sont les politiques proposées, actives et historiques?

Chaque système StorageGRID doit disposer d'une règle ILM active. Un système StorageGRID peut également avoir une proposition de règle ILM et tout nombre de règles historiques.

Lorsque vous créez une règle ILM, vous créez une proposition de règle en sélectionnant une ou plusieurs règles ILM et en les organisant dans un ordre spécifique. Après avoir simulé la stratégie proposée pour confirmer son comportement, vous l'activez pour créer la stratégie active.

Lorsque vous activez une nouvelle règle ILM, StorageGRID utilise cette règle pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Les objets existants peuvent être déplacés vers de nouveaux emplacements lorsque les règles ILM de la nouvelle règle sont mises en œuvre.

L'activation de la stratégie proposée fait de la stratégie précédemment active une stratégie historique. Les règles ILM historiques ne peuvent pas être supprimées.



Informations associées

[Création d'une règle ILM](#)

Définition d'une règle ILM

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 règle correspond aux métadonnées d'un objet, les instructions de la règle déterminent les actions qu'effectue StorageGRID pour copier et stocker cet objet.

Les règles ILM définissent :

- Les objets à stocker. Une règle peut s'appliquer à tous les objets ou vous pouvez spécifier des filtres pour identifier les objets auxquels une règle s'applique. Par exemple, une règle ne peut s'appliquer qu'aux objets associés à certains comptes de locataire, à des compartiments S3 spécifiques, à des conteneurs Swift ou à des valeurs de métadonnées spécifiques.
- Type et emplacement de stockage. Les objets peuvent être stockés sur des nœuds de stockage, dans des pools de stockage cloud ou sur des nœuds d'archivage.
- Le type de copie d'objet effectuée. Les copies peuvent être répliquées ou codées en fonction de l'effacement.
- Pour les copies répliquées, le nombre de copies effectuées.
- Pour les copies avec code d'effacement, le schéma de code d'effacement utilisé.
- Évolution au fil du temps vers l'emplacement de stockage et le type de copies d'un objet
- La protection des données objet lors de l'ingestion des objets dans la grille (placement synchrone ou double allocation).

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

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'entrée d'une règle définit ce qui se passe lorsqu'un client S3 ou Swift enregistre un objet dans la grille. 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.

Définition du filtrage des règles ILM

Lorsque vous créez une règle ILM, vous spécifiez des filtres pour identifier les objets auxquels la règle s'applique.

Dans le cas le plus simple, une règle 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. Les filtres de base de la page Define Basics de l'assistant Create ILM Rule vous permettent d'appliquer une règle à des comptes de locataire spécifiques, des compartiments S3 spécifiques, des conteneurs Swift, ou les deux.

Create ILM Rule
Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Select tenant accounts or enter tenant IDs

Bucket Name

matches all

▼

Value

[Advanced filtering...](#) (0 defined)

Cancel

Next

Ces 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.

La page **Advanced Filtering** de l'assistant Create ILM Rule vous donne 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)

- Région de compartiment S3 (contrainte d'emplacement)
- Taille de l'objet
- Métadonnées d'utilisateur
- Balises d'objet S3

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 également combiner des filtres de base et avancés 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 locataire pour isoler les enregistrements de chaque service, tout en utilisant des filtres avancés dans chaque règle pour identifier le type spécifique d'objets auquel la règle s'applique.

Instructions de placement de 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 l'icône du signe plus **+** pour ajouter plusieurs lignes pour cette période.
- Pour placer des objets à des emplacements différents dans des périodes différentes, sélectionnez le bouton **Ajouter** pour ajouter la période suivante. Spécifiez ensuite une ou plusieurs lignes dans la période.

L'exemple montre la page définir des Placements de l'assistant Créer une règle ILM.

From day store for days
Add Remove

Type replicated Location DC1 DC2 Add Pool Copies + ×

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Type erasure coded Location All 3 sites (6 plus 3) Copies 1 + ×

From day store forever
Add Remove

Type replicated Location Archive Add Pool Copies Temporary location -- Optional -- 2 + ×

1	La première instruction de placement comporte deux lignes pour la première année : 1. La première ligne crée deux copies d'objets répliquées sur deux sites de data Center. 2. La seconde ligne crée une copie avec code d'effacement de 6 + 3 sur trois sites de data Center.
2	La seconde instruction de placement crée deux copies archivées au bout d'un an et les conserve indéfiniment.

Lorsque vous définissez l'ensemble des instructions de placement pour une règle, vous devez vous assurer qu'au moins une instruction de placement commence au jour 0, qu'il n'y a pas d'écart entre les périodes que vous avez définies, et que l'instruction de placement final continue soit indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

À chaque expiration de la règle, les instructions de placement de contenu pour la période suivante sont appliquées. De nouvelles copies d'objet sont créées et les copies inutiles sont supprimées.

Exemple de règle ILM

Cet exemple de règle ILM s'applique aux objets appartenant au locataire A. Il effectue deux copies répliquées de ces objets et stocke chaque copie sur un autre site. Les deux copies sont conservées « pour toujours », ce qui signifie que StorageGRID ne les supprimera pas automatiquement. À la place, StorageGRID les conserve jusqu'à leur suppression par une demande de suppression de client ou avant l'expiration d'un cycle de vie de compartiment.

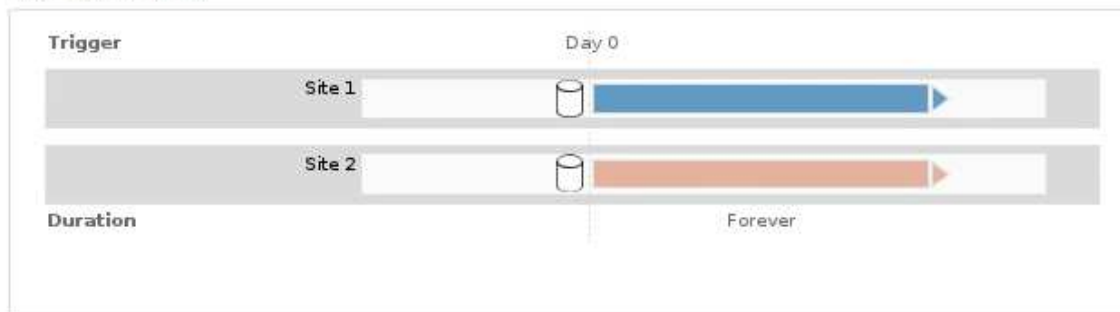
Cette règle utilise l'option équilibrée pour le comportement d'ingestion : l'instruction de placement sur deux sites est appliquée dès que le locataire A enregistre un objet dans StorageGRID, à moins qu'il ne soit pas possible de faire immédiatement les deux copies nécessaires. Par exemple, si le site 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.

Two copies at two sites for Tenant A

Description: Applies only to Tenant A
Ingest Behavior: Balanced
Tenant Accounts: Tenant A (34176783492629515782)
Reference Time: Ingest Time
Filtering Criteria:

Matches all objects.

Retention Diagram:



Informations associées

- [Options de protection des données pour l'ingestion](#)
- [Qu'est-ce qu'un pool de stockage](#)
- [Définition d'un pool de stockage cloud](#)

Créez des classes de stockage, des pools de stockage, des profils EC et des régions

Créer et attribuer des notes de stockage

Les niveaux de stockage identifient le type de stockage utilisé par un nœud de stockage. Vous pouvez créer des classes de stockage si vous souhaitez que des règles ILM placent certains objets sur certains nœuds de stockage plutôt que sur tous les nœuds du site. Vous pouvez, par exemple, stocker certains objets sur les nœuds de stockage les plus rapides, comme les appliances de stockage 100 % Flash StorageGRID.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si vous utilisez plusieurs types de stockage, vous pouvez éventuellement créer une note de stockage pour identifier chaque type. La création de nuances de stockage vous permet de sélectionner un type spécifique de

nœud de stockage lors de la configuration de pools de stockage.

Si la qualité de stockage n'est pas problématique (par exemple, tous les nœuds de stockage sont identiques), vous pouvez ignorer cette procédure et utiliser la qualité de stockage par défaut de tous les nœuds de stockage lors de la configuration des pools de stockage.

Lorsque vous ajoutez un nouveau nœud de stockage dans une extension, celui-ci est ajouté à la classe de stockage par défaut de tous les nœuds de stockage. Par conséquent :

- Si une règle ILM utilise un pool de stockage de cette catégorie pour tous les nœuds de stockage, le nouveau nœud peut être utilisé immédiatement après la fin de l'extension.
- Si une règle ILM utilise un pool de stockage avec une note de stockage personnalisée, le nouveau nœud ne sera utilisé qu'après avoir attribué manuellement la note de stockage personnalisée au nœud, comme décrit ci-dessous.

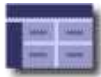


Lorsque vous créez des notes de stockage, ne créez pas plus de notes que nécessaire. Par exemple, ne créez pas une note de stockage pour chaque nœud de stockage. Attribuez plutôt chaque catégorie de stockage à deux nœuds ou plus. Des types de stockage attribués à un seul nœud peuvent entraîner des backlog ILM si ce nœud est indisponible.

Étapes

1. Sélectionnez **ILM grades de stockage**.
2. Créer une note de stockage :
 - a. Pour chaque note de stockage que vous devez définir, sélectionnez **Insérer**  pour ajouter une ligne et saisir une étiquette pour la note de stockage.

La note de stockage par défaut ne peut pas être modifiée. Il est réservé aux nouveaux nœuds de stockage ajoutés lors de l'extension d'un système StorageGRID.



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

- a. Pour modifier une note de stockage existante, sélectionnez **Modifier** et modifiez l'étiquette si nécessaire.



Vous ne pouvez pas supprimer de notes de stockage.

- b. Sélectionnez **appliquer les modifications**.

Ces classes de stockage sont désormais disponibles pour l'affectation aux nœuds de stockage.

3. Attribuer une note de stockage à un nœud de stockage :

- a. Pour le service LDR de chaque nœud de stockage, sélectionnez **Edit** et sélectionnez un grade de stockage 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 après l'activation de la politique ILM. Si l'affectation est modifiée, les données sont stockées selon le nouveau niveau de stockage.

- a. Sélectionnez **appliquer les modifications**.

Configurer les pools de stockage

Qu'est-ce qu'un pool de stockage

Un pool de stockage est un groupe logique de nœuds de stockage ou de nœuds d'archivage. Vous configurez des pools de stockage afin de déterminer l'emplacement où le système StorageGRID stocke les données d'objet et le type de stockage utilisé.

Les pools de stockage ont deux attributs :

- **Stockage** : pour les nœuds de stockage, les performances relatives du stockage de support.
- **Site** : le centre de données où les objets seront stockés.

Les pools de stockage sont utilisés dans les règles ILM pour déterminer l'emplacement de stockage des données d'objet. Lorsque vous configurez des règles ILM pour la réplication, vous sélectionnez un ou plusieurs pools de stockage incluant des nœuds de stockage ou des nœuds d'archivage. Lorsque vous créez des profils de code d'effacement, vous sélectionnez un pool de stockage incluant des nœuds de stockage.

Instructions pour la création de pools de stockage

Lorsque vous configurez et utilisez des pools de stockage, suivez ces instructions.

Instructions pour tous les pools de stockage

- StorageGRID inclut un pool de stockage par défaut, tous les nœuds de stockage, qui utilise le site par défaut, tous les sites et la qualité de stockage par défaut, tous les nœuds de stockage. Le pool de stockage tous les nœuds de stockage est automatiquement mis à jour à chaque ajout de nouveaux sites de data Center.



L'utilisation du pool de stockage tous les nœuds de stockage ou du site tous les sites n'est pas recommandée car ces éléments sont automatiquement mis à jour pour inclure les nouveaux sites que vous ajoutez à une extension, ce qui peut ne pas être le comportement que vous voulez. Avant d'utiliser le pool de stockage tous les nœuds de stockage ou le site par défaut, lisez attentivement les instructions relatives aux copies répliquées et codées par effacement.

- 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.

Instructions relatives aux pools de stockage utilisés pour les copies répliquées

- Créez un pool de stockage différent pour chaque site. Spécifiez ensuite un ou plusieurs pools de stockage spécifiques au site dans les instructions de placement pour chaque règle. 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 pour le nouveau site. Ensuite, mettez à jour les règles ILM pour contrôler les objets qui sont stockés sur le nouveau site.
- En général, n'utilisez pas le pool de stockage par défaut, tous les nœuds de stockage ou tout pool de stockage incluant le site par défaut, tous les sites.

Instructions relatives aux pools de stockage utilisés pour les copies avec code d'effacement

- Vous ne pouvez pas utiliser les nœuds d'archivage pour les données avec code d'effacement.
- Le nombre de sites et de nœuds de stockage du pool détermine les schémas de code d'effacement disponibles.
- Si un pool de stockage comprend seulement deux sites, vous ne pouvez pas utiliser ce pool de stockage pour le codage d'effacement. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage possédant deux sites.
- En général, n'utilisez pas le pool de stockage par défaut, tous les nœuds de stockage ou tout pool de stockage incluant le site par défaut, tous les sites d'un profil de code d'effacement.



Si votre grid ne contient qu'un seul site, vous ne pouvez pas utiliser le pool de stockage tous les nœuds de stockage ou le site par défaut de tous les sites dans un profil de code d'effacement. Ce comportement empêche le profil de code d'effacement de devenir non valide si un second site est ajouté.

- Si vous avez des besoins élevés en débit, il est déconseillé de créer un pool de stockage incluant 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 réalisables d'entrée et de récupération d'objet (lorsque stricte ou équilibré sont sélectionnés comme comportement d'ingestion) ou risque d'entraîner des arriérés de file d'attente ILM (lorsque la fonction de double validation est sélectionnée comme comportement d'ingestion).
- 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.

Instructions relatives aux pools de stockage utilisés pour les copies archivées

- Vous ne pouvez pas créer de pool de stockage incluant à la fois les nœuds de stockage et les nœuds d'archivage. Les copies archivées nécessitent un pool de stockage incluant uniquement les nœuds d'archivage.
- Lorsque vous utilisez un pool de stockage incluant des nœuds d'archivage, vous devez également conserver au moins une copie répliquée ou codée d'effacement dans un pool de stockage incluant des nœuds de stockage.
- Si le paramètre global de verrouillage d'objet S3 est activé et que vous créez une règle ILM conforme, vous ne pouvez pas utiliser un pool de stockage incluant les nœuds d'archivage. Voir les instructions de gestion des objets avec le verrouillage d'objet S3.
- Si le type cible d'un nœud d'archivage est Cloud Tiering - simple Storage Service (S3), le nœud d'archivage doit se trouver dans son propre pool de stockage. Voir [Administrer StorageGRID](#).

Informations associées

- [Qu'est-ce que la réplication](#)
- [Qu'est-ce que le code d'effacement](#)
- [En quoi consiste les schémas de code d'effacement](#)
- [Utilisation de plusieurs pools de stockage pour la réplication intersites](#)

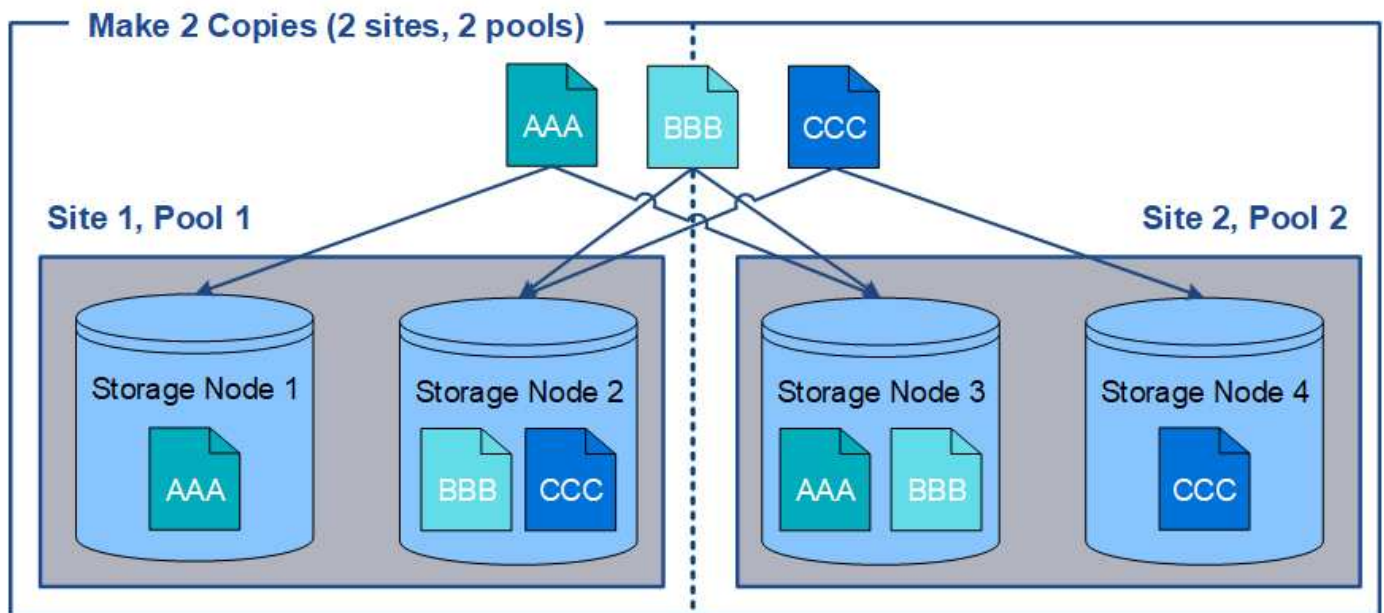
Utilisation de plusieurs pools de stockage pour la réplication intersites

Si votre déploiement StorageGRID inclut plusieurs sites, vous pouvez activer la protection contre la perte de site en créant un pool de stockage pour chaque site et en spécifiant les deux pools de stockage dans les instructions de placement de la règle. Par exemple, si vous configurez une règle ILM pour effectuer deux copies répliquées et spécifier des pools de stockage sur deux sites, une copie de chaque objet sera placée sur chaque site. Si vous configurez une règle pour faire deux copies et spécifier trois pools de stockage, les copies sont distribuées pour équilibrer l'utilisation des disques entre les pools de stockage, tout en vous assurant que les deux copies sont stockées sur différents sites.

L'exemple suivant illustre ce qui peut se produire si une règle ILM place les copies d'objet répliquées dans un

pool de stockage unique contenant des nœuds de stockage provenant de deux sites. Étant donné que le système utilise les nœuds disponibles dans le pool de stockage lorsqu'il place les copies répliquées, il peut placer toutes les copies de certains objets au sein d'un seul site. Dans cet exemple, le système a stocké deux copies de l'objet AAA sur les nœuds de stockage du site 1 et deux copies de l'objet CCC sur les nœuds de stockage du site 2. Seul l'objet BBB est protégé si l'un des sites tombe en panne ou devient inaccessible.

Cet exemple montre en revanche comment les objets sont stockés lorsque vous utilisez plusieurs pools de stockage. Dans l'exemple, la règle ILM indique que deux copies répliquées de chaque objet doivent être créées, et que ces copies sont distribuées sur deux pools de stockage. Chaque pool de stockage contient tous les nœuds de stockage sur un site. Étant donné que une copie de chaque objet est stockée sur chaque site, les données d'objet sont protégées contre les pannes au niveau du site ou de ce site, sans aucune accessibilité.



Lorsque vous utilisez plusieurs pools de stockage, gardez les règles suivantes à l'esprit :

- Si vous créez n copies, vous devez ajouter n pools de stockage ou plus. Par exemple, si une règle est configurée pour faire trois copies, vous devez spécifier trois pools de stockage ou plus.
- 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, le système distribue les copies pour maintenir l'utilisation du disque entre les pools équilibrés et pour s'assurer que deux copies ou plus ne sont pas stockées dans le même pool de stockage.
- 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.

Utiliser un pool de stockage comme emplacement temporaire (obsolète)

Lorsque vous créez une règle ILM avec un placement d'objets incluant un pool de stockage, vous êtes invité à spécifier un second pool de stockage à utiliser comme emplacement temporaire.

Les sites temporaires sont obsolètes et seront supprimés dans une version ultérieure. Vous ne devez pas

sélectionner un pool de stockage comme emplacement temporaire pour une nouvelle règle ILM.



Si vous sélectionnez le comportement d'entrée strict (étape 3 de l'assistant Créer une règle ILM), l'emplacement temporaire est ignoré.

Informations associées

[Options de protection des données pour l'ingestion](#)

Créer un pool de stockage

Vous créez des pools de stockage afin de déterminer où le système StorageGRID stocke les données d'objet et le type de stockage utilisé. Chaque pool de stockage comprend un ou plusieurs sites et une ou plusieurs catégories de stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue les instructions relatives à la création de pools de stockage.

Description de la tâche

Les pools de stockage déterminent l'emplacement de stockage des données d'objet. Le nombre de pools de stockage dont vous avez besoin dépend du nombre de sites de votre grid et des types de copies que vous souhaitez : répliquées ou avec code d'effacement.

- Pour la réplication et le code d'effacement à un seul site, créez un pool de stockage pour chaque site. Par exemple, si vous souhaitez stocker les copies d'objets répliquées sur trois sites, créez trois pools de stockage.
- Pour le codage d'effacement sur trois sites ou plus, créez un pool de stockage comprenant une entrée pour chaque site. Par exemple, si vous souhaitez effacement d'objets de code sur trois sites, créez un pool de stockage. Sélectionnez l'icône plus  pour ajouter une entrée pour chaque site.



N'incluez pas le site par défaut tous les sites dans un pool de stockage qui sera utilisé dans un profil de code d'effacement. Ajoutez plutôt une entrée distincte au pool de stockage pour chaque site qui stocke les données codées d'effacement. Voir [cette étape](#) par exemple.

- Si vous disposez de plusieurs niveaux de stockage, ne créez pas de pool de stockage incluant différentes catégories de stockage sur un même site. Voir la [Instructions pour la création de pools de stockage](#).

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools (pools de stockage) s'affiche et répertorie tous les pools de stockage définis.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

Create

Edit

Remove

View Details

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create	✎ Edit	✕ Remove	Clear Error

No Cloud Storage Pools found.

La liste inclut le pool de stockage par défaut du système, tous les nœuds de stockage, qui utilise le site par défaut du système, tous les sites et la qualité de stockage par défaut, tous les nœuds de stockage.



Le pool de stockage tous les nœuds de stockage est automatiquement mis à jour lors de l'ajout de nouveaux sites de data Center. Il n'est donc pas recommandé d'utiliser ce pool de stockage dans les règles ILM.

2. Pour créer un nouveau pool de stockage, sélectionnez **Créer**.

La boîte de dialogue Créer un pool de stockage s'affiche.

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, click + to add each site to a single storage pool.
- Do not add more than one storage grade for a single site.

Name

Site

-- Choose One --

Storage Grade

All Storage Nodes

+

Viewing Storage Pool -

Site Name	Archive Nodes	Storage Nodes

Cancel

Save

3. Entrez un nom unique pour le pool de stockage.

Utilisez un nom qui sera facilement identifié lors de la configuration des profils de code d'effacement et des règles ILM.

4. Dans la liste déroulante **site**, sélectionnez un site pour ce pool de stockage.

Lorsque vous sélectionnez un site, le nombre de nœuds de stockage et de nœuds d'archivage dans le tableau est automatiquement mis à jour.

En général, n'utilisez pas le site par défaut tous les sites dans aucun 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 **grade de stockage**, sélectionnez le type de stockage à utiliser si une règle ILM utilise ce pool de stockage.

La qualité de stockage tous les nœuds de stockage par défaut inclut tous les nœuds de stockage du site sélectionné. Le niveau de stockage par défaut des nœuds d'archivage inclut tous les nœuds d'archivage du site sélectionné. Si vous avez créé des notes de stockage supplémentaires pour les nœuds de stockage de votre grille, elles sont répertoriées dans la liste déroulante.

6. si vous souhaitez utiliser le pool de stockage dans un profil de code d'effacement multisite, sélectionnez **+** pour ajouter une entrée pour chaque site au pool de stockage.

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, select + to add each site to a single storage pool.
- Do not select more than one storage grade for a single site.

Name	All 3 Sites for Erasure Coding			
Site	Data Center 1	Storage Grade	All Storage Nodes	✕
Site	Data Center 2	Storage Grade	All Storage Nodes	✕
Site	Data Center 3	Storage Grade	All Storage Nodes	+ ✕

Viewing Storage Pool - All 3 Sites for Erasure Coding

Site Name	Archive Nodes	Storage Nodes
Data Center 1	0	3
Data Center 2	0	3
Data Center 3	0	3

You are creating a multi-site storage pool, which should not be used for replication or single-site erasure coding.

Cancel

Save



Vous ne pouvez pas créer d'entrées dupliquées ou créer un pool de stockage qui inclut à la fois la qualité de stockage **Archive Nodes** et toute classe de stockage contenant des nœuds de stockage.

Vous êtes averti si vous ajoutez plus d'une entrée pour un site mais avec des niveaux de stockage différents.

Pour supprimer une entrée, sélectionnez ✕.

7. Lorsque vous êtes satisfait de vos sélections, sélectionnez **Enregistrer**.

Le nouveau pool de stockage est ajouté à la liste.

Afficher les détails du pool de stockage

Vous pouvez afficher les détails d'un pool de stockage pour déterminer où le pool de stockage est utilisé et pour voir quels nœuds et niveaux de stockage sont inclus.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche. Cette page répertorie tous les pools de stockage définis.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit ✕ Remove View Details					
	Name ?	Used Space ?	Free Space ?	Total Capacity ?	ILM Usage ?
	All Storage Nodes	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule
	DC1	621.77 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
	DC2	675.82 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
	DC3	578.95 KB	932.42 GB	932.42 GB	Used in 1 ILM rule
	All 3 Sites	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule and 1 EC profile
	Archive	—	—	—	—

Displaying 6 storage pools.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit ✕ Remove Clear Error			
No Cloud Storage Pools found.			

Le tableau contient les informations suivantes pour chaque pool de stockage incluant les nœuds de stockage :

- **Nom** : nom d'affichage unique du pool de stockage.
- **Espace utilisé** : espace actuellement utilisé pour stocker des objets dans le pool de stockage.
- **Espace libre** : espace disponible pour stocker des objets dans le pool de stockage.

- **Capacité totale** : la taille du pool de stockage, qui équivaut 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 non utilisé, ou être utilisé dans une ou plusieurs règles ILM, les profils de code d'effacement, ou les deux.



Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé.

2. Pour afficher les détails d'un pool de stockage spécifique, sélectionnez son bouton radio et sélectionnez **Afficher les détails**.

Le modal Storage Pool Details s'affiche.

3. Consultez l'onglet **nœuds inclus** pour en savoir plus sur les nœuds de stockage ou les nœuds d'archivage inclus dans le pool de stockage.

Storage Pool Details - DC1			
Nodes Included		ILM Usage	
Number of Nodes:		3	
Site - Storage Grade:		DC1 - All Storage Nodes	
Node Name	Site Name	Used (%) ?	↑↓
DC1-S3	DC1	0.000%	
DC1-S2	DC1	0.000%	
DC1-S1	DC1	0.000%	
			Close

Le tableau inclut les informations suivantes pour chaque nœud :

- Nom du nœud
- Nom du site
- Utilisé (%) : pour les nœuds de stockage, pourcentage de l'espace total utilisable pour les données d'objet qui ont été utilisées. Cette valeur n'inclut pas les métadonnées d'objet.



La même valeur utilisée (%) est également indiquée dans le tableau stockage utilisé - données d'objet pour chaque nœud de stockage (sélectionnez **NOEUDS nœud de stockage Storage**).

4. Sélectionnez l'onglet **ILM usage** pour déterminer si le pool de stockage est actuellement utilisé dans les règles ILM ou les profils de code d'effacement.

Dans cet exemple, le pool de stockage DC1 est utilisé dans trois règles ILM : deux règles qui figurent dans la politique ILM active et une règle qui ne fait pas partie de la politique active.

Storage Pool Details - DC1

Nodes Included

ILM Usage

ILM Rules Using the Storage Pool

The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.

- 3 copies for Account01
- 2 copies for smaller objects

1 ILM rule that is not in the active ILM policy uses this storage pool.

If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the [ILM Rules page](#).

EC Profiles Using the Storage Pool

No Erasure Coding profiles use this storage pool.

Close



Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé dans une règle ILM.

Dans cet exemple, le pool de stockage 3 sites est utilisé dans un profil de code d'effacement. Ensuite, ce profil de code d'effacement est utilisé par une règle ILM de la politique ILM active.

Storage Pool Details - All 3 Sites

Nodes Included

ILM Usage

ILM Rules Using the Storage Pool

The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.

- EC larger objects

If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the [ILM Rules page](#).

EC Profiles Using the Storage Pool

The following Erasure Coding profiles use this storage pool.

Profile Name	Profile Status ?
6 plus 3	Used in 1 ILM Rule

Close



Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé dans un profil de code d'effacement.

5. Vous pouvez également consulter la page **ILM Rules** pour en savoir plus sur les règles qui utilisent le pool de stockage et les gérer.

Voir les instructions d'utilisation des règles ILM.

6. Lorsque vous avez terminé d'afficher les détails du pool de stockage, sélectionnez **Fermer**.

Informations associées

Utilisation des règles ILM et des règles ILM

Modifier le pool de stockage

Vous pouvez modifier un pool de stockage pour modifier son nom ou mettre à jour des sites et des notes de stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue les instructions relatives à la création de pools de stockage.
- 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 une nouvelle qualité de stockage à un pool de stockage utilisé dans la règle ILM active, sachez que les nœuds de stockage de la nouvelle qualité ne sont pas automatiquement utilisés. Pour forcer StorageGRID à utiliser une nouvelle qualité de stockage, vous devez activer une nouvelle règle ILM après avoir enregistré le pool de stockage modifié.

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche.

2. Sélectionnez le bouton radio du pool de stockage que vous souhaitez modifier.

Vous ne pouvez pas modifier le pool de stockage tous les nœuds de stockage.

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 n'avez pas la possibilité de modifier le site ou la qualité de stockage si le pool de stockage est utilisé dans un profil de code d'effacement, ce qui entraînerait la non-validité du schéma de code d'effacement. Par exemple, si un pool de stockage utilisé dans un profil Erasure Coding inclut actuellement une classe de stockage avec un seul site, vous ne pouvez pas utiliser une classe de stockage avec deux sites, car la modification rendrait le schéma de code d'effacement non valide.

6. Sélectionnez **Enregistrer**.

Une fois que vous avez terminé

Si vous avez ajouté une nouvelle classe de stockage à un pool de stockage utilisé dans la règle ILM active, activez une nouvelle règle ILM pour forcer StorageGRID à utiliser la nouvelle version du stockage. Par exemple, clonez votre règle ILM existante, puis activez le clone.

Retirez un pool de stockage

Vous pouvez supprimer un pool de stockage qui n'est pas utilisé.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche.

2. Consultez la colonne utilisation 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. Selon les besoins, sélectionnez **View Details ILM usage** pour déterminer où un pool de stockage est utilisé.

3. Si le pool de stockage que vous souhaitez supprimer n'est pas utilisé, sélectionnez la case d'option.
4. Sélectionnez **Supprimer**.
5. Sélectionnez **OK**.

Utilisation des pools de stockage cloud

Définition d'un pool de stockage cloud

Un pool de stockage cloud permet d'utiliser des règles ILM pour déplacer des données d'objet en dehors de votre système StorageGRID. Par exemple, vous pouvez déplacer des objets peu utilisés vers un stockage cloud à moindre coût, comme Amazon S3 Glacier, S3 Glacier Deep Archive ou le Tier d'accès à l'archivage dans le stockage Microsoft Azure Blob. Vous pouvez également conserver une sauvegarde dans le cloud des objets StorageGRID pour améliorer la reprise d'activité.

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Pour stocker des objets à l'un ou l'autre des emplacements, sélectionnez le pool lors de la création des instructions de placement pour une règle ILM. Toutefois, alors que les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment externe (S3) ou d'un conteneur (stockage Azure Blob Storage).

Le tableau suivant compare les pools de stockage avec les pools de stockage cloud et présente les similarités et les différences générales.

	Pool de stockage	Pool de stockage cloud
Comment est-elle créée ?	Utilisation de l'option ILM Storage pools dans Grid Manager. Vous devez configurer les classes de stockage avant de pouvoir créer le pool de stockage.	Utilisation de l'option ILM Storage pools dans Grid Manager. Vous devez configurer le compartiment ou le conteneur externe avant de pouvoir créer le pool de stockage cloud.
Combien de pools pouvez-vous créer ?	Illimitée.	Jusqu'à 10.
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage ou d'archivage dans StorageGRID.	Dans un compartiment Amazon S3 ou un conteneur de stockage Azure Blob externe au système StorageGRID. Si le pool de stockage cloud est un compartiment Amazon S3 : • Vous pouvez configurer un cycle de vie de compartiment pour la transition des objets vers un stockage à long terme à faible coût, comme Amazon S3 Glacier ou S3 Glacier Deep Archive. Le système de stockage externe doit prendre en charge la classe de stockage Glacier et l'API S3 POST-restauration objet. • Vous pouvez créer des pools de stockage cloud à utiliser avec AWS commercial Cloud Services (C2S), qui prend en charge la région secrète AWS. Si le pool de stockage cloud est un conteneur de stockage Azure Blob, StorageGRID transfère l'objet vers le Tier d'archivage. Remarque : en général, ne configurez pas la gestion du cycle de vie du stockage Azure Blob Storage pour le conteneur utilisé pour un pool de stockage cloud. Les opérations DE restauration POST-objet des objets dans le pool de stockage cloud peuvent être affectées par le cycle de vie configuré.
Quels sont les contrôles du placement des objets ?	Règle ILM de la politique ILM active.	Règle ILM de la politique ILM active.

	Pool de stockage	Pool de stockage cloud
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

Cycle de vie d'un objet de pool de stockage cloud

Avant d'implémenter les pools de stockage cloud, vérifiez le cycle de vie des objets stockés dans chaque type de pool de stockage cloud.

- [S3 : cycle de vie d'un objet de pool de stockage cloud](#)
- [Azure : cycle de vie d'un objet de pool de stockage cloud](#)

S3 : cycle de vie d'un objet de pool de stockage cloud

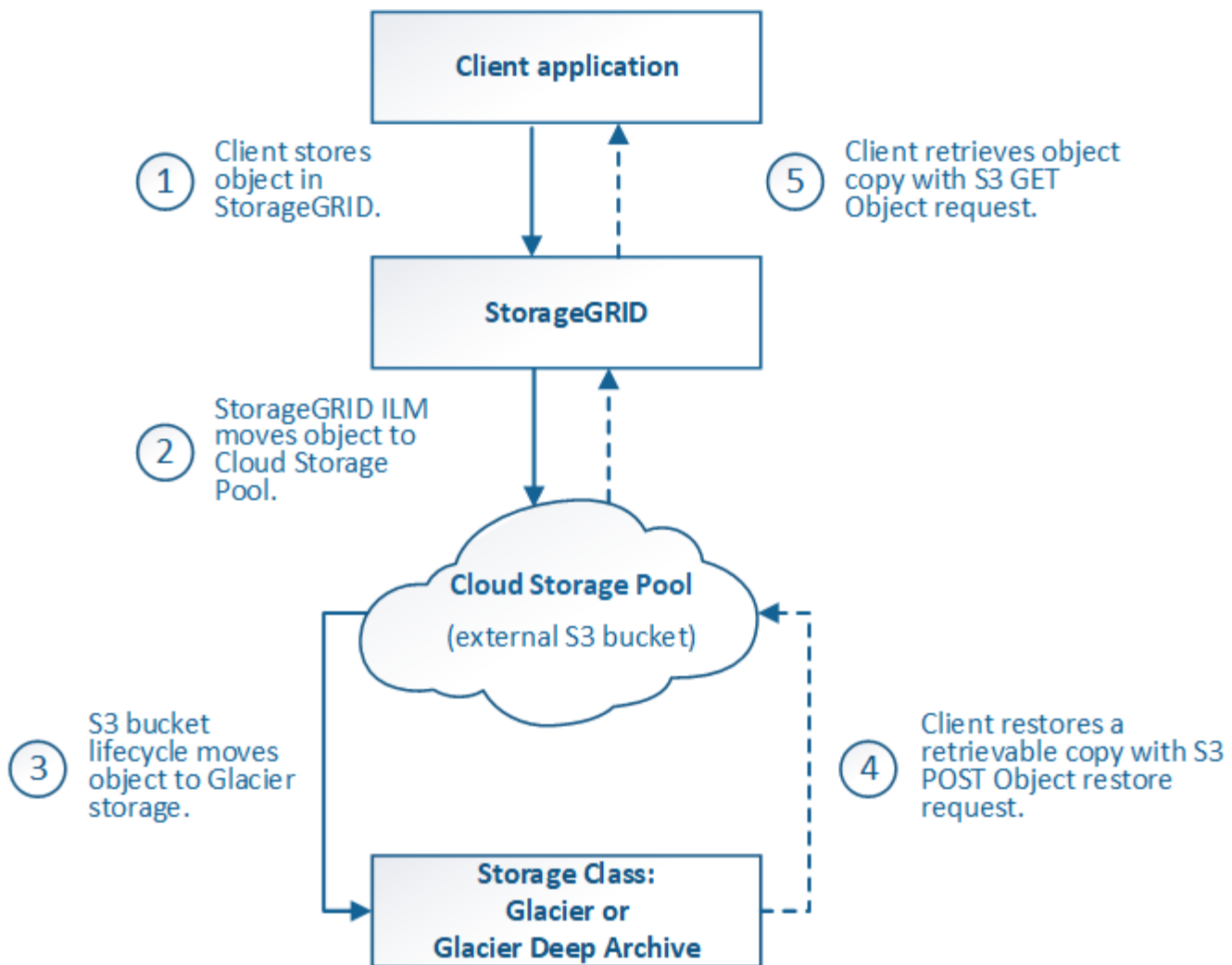
La figure représente les étapes du cycle de vie d'un objet stocké dans un pool de stockage cloud S3.



Dans la figure et les explications, « Glacier » désigne à la fois la classe de stockage Glacier et la classe de stockage Glacier Deep Archive, à une exception près : la classe de stockage Glacier Deep Archive ne prend pas en charge le niveau de restauration accéléré. Seule la récupération en bloc ou standard est prise en charge.



Google Cloud Platform (GCP) prend en charge la récupération d'objets à partir d'un stockage à long terme sans nécessiter de POST-restauration.



1. Objet stocké dans StorageGRID

Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. Objet déplacé vers le pool de stockage cloud S3

- Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud S3 en tant qu'emplacement, StorageGRID déplace l'objet vers le compartiment S3 externe spécifié par le pool de stockage cloud.
- Lorsque l'objet a été déplacé vers le pool de stockage cloud S3, l'application client peut la récupérer à l'aide d'une requête d'objet GET S3 de StorageGRID, à moins que l'objet n'ait été transféré vers le stockage Glacier.

3. L'objet a été transféré vers Glacier (état non récupérable)

- L'objet peut également être transféré vers le stockage Glacier. Par exemple, un compartiment S3 externe peut utiliser la configuration du cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après quelques jours.



Si vous souhaitez effectuer la transition des objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe. Pour ce faire, vous devez utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API S3 POST-restauration objet.



N'utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le stockage Glacier S3. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).

- Lors de la transition, l'application client peut utiliser une requête objet TÊTE S3 pour contrôler l'état de l'objet.

4. Objet restauré à partir du stockage Glacier

Lorsqu'un objet est transféré vers le stockage Glacier, l'application client peut émettre une demande de restauration APRÈS objet S3 pour restaurer une copie récupérable dans le pool de stockage cloud S3. La demande spécifie le nombre de jours pendant lesquels la copie doit être disponible dans le pool de stockage cloud et le Tier d'accès aux données à utiliser pour l'opération de restauration (accéléré, Standard ou en bloc). Lorsque la date d'expiration de la copie récupérable est atteinte, la copie est automatiquement renvoyée à un état non récupérable.



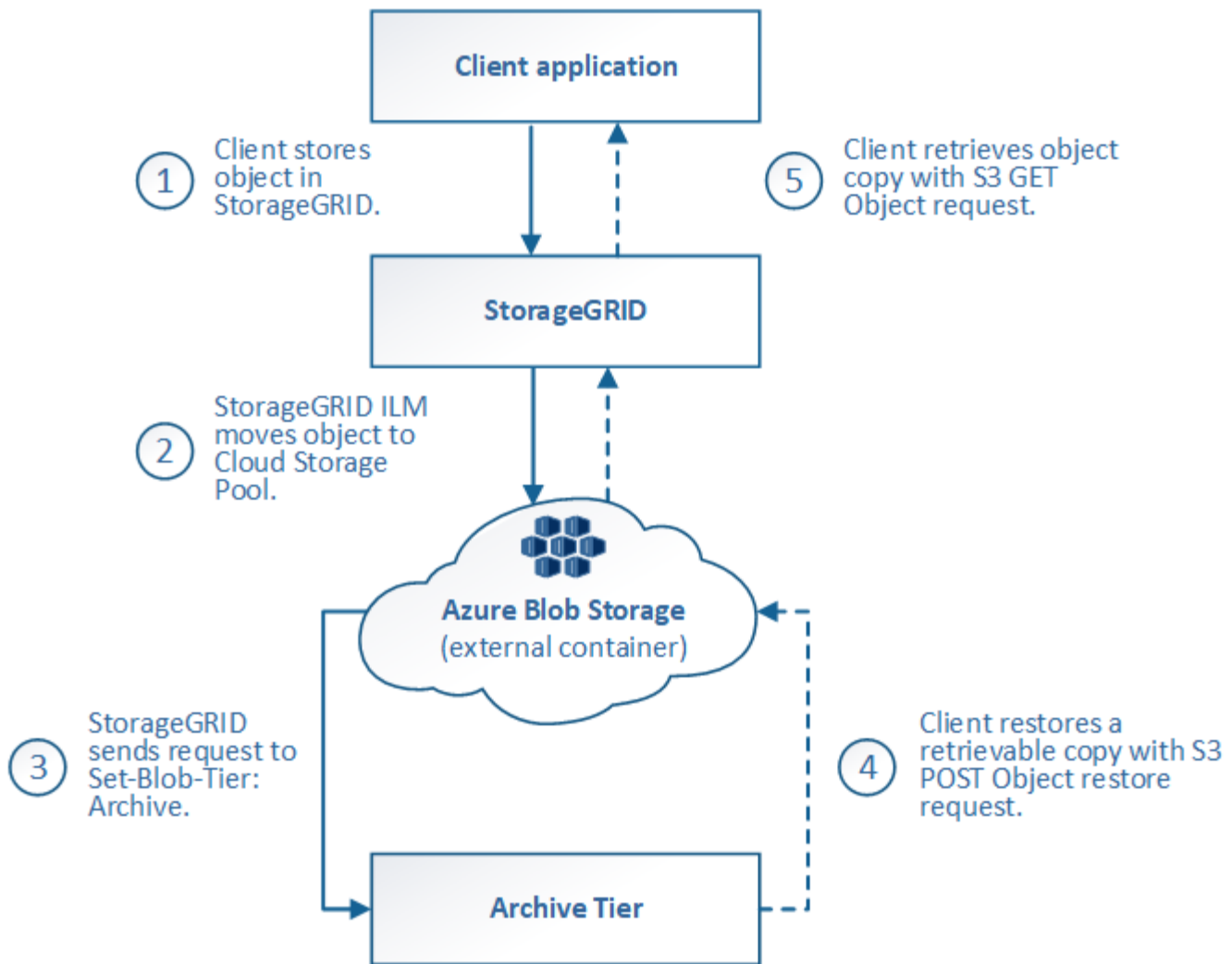
Si une ou plusieurs copies de l'objet existent également sur les nœuds de stockage dans StorageGRID, il n'est pas nécessaire de restaurer l'objet à partir de Glacier à l'aide d'une demande DE restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

5. Objet récupéré

Une fois qu'un objet a été restauré, l'application client peut émettre une requête GET Object pour récupérer l'objet restauré.

Azure : cycle de vie d'un objet de pool de stockage cloud

La figure représente les étapes du cycle de vie d'un objet stocké dans un pool de stockage cloud Azure.



1. Objet stocké dans StorageGRID

Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. Objet déplacé vers Azure Cloud Storage Pool

Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud Azure comme emplacement, StorageGRID déplace l'objet vers le conteneur de stockage Azure Blob externe spécifié par le pool de stockage cloud



N'utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le niveau d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).

3. L'objet a été transféré au niveau Archive (état non récupérable)

Immédiatement après le déplacement de l'objet vers le pool de stockage cloud Azure, StorageGRID transfère automatiquement l'objet vers le Tier d'archivage du stockage Azure Blob.

4. Objet restauré à partir du niveau d'archive

Si un objet a été migré vers le Tier d'archivage, l'application client peut lancer une demande de restauration S3 POST-objet pour restaurer une copie récupérable dans le pool de stockage cloud Azure.

Lorsqu'StorageGRID reçoit le POST-restauration d'objet, il transfère temporairement l'objet vers le Tier Azure Blob Storage Cool. Dès que la date d'expiration de la requête DE restauration POST-objet est atteinte, StorageGRID retransfère l'objet vers le niveau d'archivage.



Si une ou plusieurs copies de l'objet existent également sur les nœuds de stockage dans StorageGRID, il n'est pas nécessaire de restaurer l'objet à partir du Tier d'accès Archive en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

5. Objet récupéré

Une fois qu'un objet a été restauré dans Azure Cloud Storage Pool, l'application client peut émettre une requête GET Object pour récupérer l'objet restauré.

Informations associées

[Utilisation de S3](#)

Quand utiliser les pools de stockage cloud

Les pools de stockage cloud offrent des avantages significatifs dans plusieurs cas d'utilisation.

Sauvegarde des données StorageGRID dans un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder des objets StorageGRID dans un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, vous pouvez utiliser les données objet du pool de stockage cloud pour transmettre les requêtes des clients. Cependant, vous devrez peut-être émettre une demande de restauration S3 POST-objet pour accéder à la copie d'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objet d'un pool de stockage cloud peuvent également être utilisées pour restaurer des données perdues à partir de StorageGRID en raison d'un volume de stockage ou d'une défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

Pour implémenter une solution de sauvegarde :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour stocker simultanément les copies d'objets sur les nœuds de stockage (en tant que copies répliquées ou avec code d'effacement) et une seule copie objet dans le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Tiering des données du 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 pools de stockage cloud si vous souhaitez hiérarchiser ou sauvegarder des données d'objet dans plusieurs clouds. Les filtres de vos règles ILM permettent de spécifier les objets qui sont stockés dans chaque pool de stockage cloud. Par exemple, vous pouvez stocker des objets à partir de certains locataires ou compartiments dans Amazon S3 Glacier et des objets à partir d'un autre locataire ou compartiments dans le stockage Azure Blob. Vous pouvez également déplacer des données entre Amazon S3 Glacier et le stockage Azure Blob. Si vous utilisez plusieurs pools de stockage cloud, n'oubliez pas qu'un objet ne peut être stocké que dans un seul pool de stockage cloud à la fois.

Pour implémenter plusieurs terminaux cloud :

1. Créez jusqu'à 10 pools de stockage cloud.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment opportun dans chaque pool de stockage cloud. Stockez par exemple des objets à partir du compartiment A dans le pool de stockage cloud A et stockez des objets à partir du compartiment B dans le pool de stockage cloud B. Stockez les objets dans Cloud Storage Pool A pendant un certain temps, puis déplacez-les vers Cloud Storage Pool B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simuler et activer la règle.

Considérations relatives aux pools de stockage cloud

Si vous envisagez d'utiliser un pool de stockage cloud pour déplacer les objets hors du système StorageGRID, vous devez étudier les critères de configuration et d'utilisation des pools de stockage cloud.

Considérations générales

- En général, le stockage d'archivage dans le cloud, comme Amazon S3 Glacier ou Azure Blob Storage, est un emplacement économique pour stocker les données d'objet. Mais le coût de la récupération des données à partir du stockage d'archivage dans le cloud est relativement élevé. Pour atteindre le coût global le plus bas, vous devez savoir quand et à quelle fréquence vous accéderez aux objets dans Cloud Storage Pool. L'utilisation d'un pool de stockage cloud est recommandée uniquement pour le contenu dont vous souhaitez accéder rarement.
- N'utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le stockage Glacier S3 ou le Tier d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).
- L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.

Informations requises pour la création d'un pool de stockage cloud

Avant de créer un pool de stockage cloud, vous devez créer un compartiment S3 externe ou le conteneur de stockage Azure Blob externe que vous utiliserez pour le pool de stockage cloud. Lorsque vous créez le pool de stockage cloud dans StorageGRID, vous devez spécifier les informations suivantes :

- Le type de fournisseur : stockage Amazon S3 ou Azure Blob.
- Si vous sélectionnez Amazon S3, que le pool de stockage cloud soit utilisé avec la région secrète AWS (**CAP (C2S Access Portal)**).
- Nom exact du godet ou du conteneur.
- Le terminal de service devait accéder au compartiment ou au conteneur.
- Pour accéder au compartiment ou au conteneur :
 - **S3** : en option, une clé d'accès et une clé secrète d'accès.
 - **C2S** : l'URL complète pour obtenir les informations d'identification temporaires du serveur CAP; un certificat d'autorité de certification de serveur, un certificat client, une clé privée pour le certificat client, et, si la clé privée est cryptée, la phrase de passe pour le déchiffrer.
 - **Stockage Azure Blob** : nom de compte et clé de compte. Ces informations d'identification doivent disposer d'une autorisation complète pour le conteneur.
- Un certificat d'autorité de certification personnalisé permet éventuellement de vérifier les connexions TLS avec le compartiment ou le conteneur.

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](#) pour permettre l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur internet.

Considérations relatives aux coûts

L'accès au stockage dans le cloud à l'aide d'un pool de stockage cloud requiert une connectivité réseau au cloud. Tenez compte des coûts de l'infrastructure réseau que vous utiliserez pour accéder au cloud et le provisionner de façon appropriée, en fonction de la quantité de données que vous prévoyez de déplacer entre StorageGRID et le cloud à l'aide du pool de stockage cloud.

Lorsque StorageGRID se connecte au terminal Cloud Storage Pool externe, plusieurs demandes de contrôle de la connectivité sont émises et les opérations nécessaires sont possibles. Un certain nombre de coûts supplémentaires seront associés à ces demandes, mais le coût de la surveillance d'un pool de stockage cloud ne doit être qu'une fraction du coût global du stockage d'objets dans S3 ou Azure.

Des coûts plus importants peuvent être encourus si vous devez déplacer des objets depuis un terminal externe

de pool de stockage dans le cloud vers StorageGRID. Les objets peuvent être redéplacés vers StorageGRID dans l'un ou l'autre de ces cas :

- La seule copie de l'objet se trouve dans un pool de stockage cloud et vous décidez de le stocker dans StorageGRID à la place. Dans ce cas, il vous suffit de reconfigurer les règles et les règles ILM. Lors de l'évaluation ILM, StorageGRID émet plusieurs demandes de récupération de l'objet à partir du pool de stockage cloud. StorageGRID crée ensuite le nombre spécifié de copies répliquées ou codées en local. Une fois que l'objet est de nouveau déplacé vers StorageGRID, la copie dans le pool de stockage cloud est supprimée.
- Les objets sont perdus en raison de la défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.



Lorsque les objets sont déplacés vers StorageGRID à partir d'un pool de stockage cloud, StorageGRID émet plusieurs requêtes vers le terminal de pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, contactez le support technique pour obtenir de l'aide pour estimer le délai et les coûts associés.

S3 : autorisations requises pour le compartiment de pool de stockage cloud

La politique de compartiment pour le compartiment S3 externe utilisé pour un pool de stockage cloud doit autoriser StorageGRID à déplacer un objet vers le compartiment, à obtenir l'état d'un objet et à restaurer un objet à partir du stockage Glacier, le cas échéant, et bien plus encore. Dans l'idéal, StorageGRID doit disposer d'un accès total au compartiment (`s3:*`) ; Cependant, si ce n'est pas possible, la politique de compartiment doit accorder les autorisations S3 suivantes à StorageGRID :

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3 : considérations sur le cycle de vie du compartiment externe

Le déplacement des objets entre le StorageGRID et le compartiment S3 externe spécifié dans le pool de stockage cloud est contrôlé par les règles ILM et la politique ILM active dans StorageGRID. À l'inverse, la transition des objets à partir du compartiment S3 externe spécifié dans le pool de stockage cloud vers Amazon S3 Glacier ou S3 Glacier Deep Archive (ou vers une solution de stockage implémentant la classe de stockage Glacier) est contrôlée par la configuration du cycle de vie de ce compartiment.

Si vous souhaitez migrer des objets depuis le pool de stockage cloud, vous devez créer la configuration de cycle de vie appropriée sur un compartiment S3 externe. Vous devez d'autre part utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API DE restauration POST-objet S3.

Supposons par exemple que vous souhaitiez que tous les objets déplacés d'StorageGRID vers le pool de

stockage cloud soient transférés immédiatement vers le stockage Amazon S3 Glacier. Vous devez créer une configuration de cycle de vie sur le compartiment S3 externe qui spécifie une seule action (**transition**) comme suit :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Cette règle consiste à basculer tous les objets de compartiment vers Amazon S3 Glacier le jour de leur création (à savoir le jour où ils ont été déplacés d'StorageGRID vers le pool de stockage cloud).



Lors de la configuration du cycle de vie du compartiment externe, n'utilisez jamais les actions **expiration** pour définir quand les objets arrivent à expiration. Les actions d'expiration entraînent la suppression des objets expirés par le système de stockage externe. Si vous tentez par la suite d'accéder à un objet expiré à partir de StorageGRID, l'objet supprimé est introuvable.

Pour migrer les objets du pool de stockage cloud vers l'archivage profond S3 Glacier (au lieu d'Amazon S3 Glacier), spécifiez `<StorageClass>DEEP_ARCHIVE</StorageClass>` pendant le cycle de vie du compartiment. Toutefois, sachez que vous ne pouvez pas utiliser le Expedited tiering pour restaurer des objets à partir d'une archive complète S3 Glacier.

Azure : considérations relatives au niveau d'accès

Lorsque vous configurez un compte de stockage Azure, vous pouvez définir le niveau d'accès par défaut sur chaud ou froid. Lorsque vous créez un compte de stockage à utiliser avec un pool de stockage cloud, vous devez utiliser le Tier actif comme niveau par défaut. Même si StorageGRID définit immédiatement le Tier sur Archive lors du déplacement d'objets vers le pool de stockage cloud, l'utilisation du paramètre par défaut de Hot garantit que vous ne serez pas facturé de frais de suppression anticipé pour les objets supprimés du Tier Cool avant le minimum de 30 jours.

Azure : gestion du cycle de vie non prise en charge

N'utilisez pas la fonctionnalité de gestion du cycle de vie du stockage Azure Blob Storage pour le conteneur utilisé avec un pool de stockage cloud. Toute interférence entre les opérations du cycle de vie du système Cloud Storage Pool.

Informations associées

- [Création d'un pool de stockage cloud](#)
- [S3 : spécifiez les détails d'authentification pour un pool de stockage cloud](#)

- [C2S S3](#) : spécification des détails d'authentification pour un pool de stockage cloud
- [Azure](#) : spécifiez les détails d'authentification pour un pool de stockage cloud

Comparaison des pools de stockage cloud et de la réplication CloudMirror

Lorsque vous commencez à utiliser les pools de stockage cloud, il peut être utile d'étudier les similarités et les différences entre les pools de stockage cloud et le service de réplication StorageGRID CloudMirror.

	Pool de stockage cloud	Service de réplication CloudMirror
Quel est l'objectif principal ?	Un pool de stockage cloud agit comme cible d'archivage. La copie d'objet du pool de stockage cloud peut être la seule copie de l'objet ou une copie supplémentaire. Par exemple, au lieu de conserver deux copies sur site, vous ne pouvez conserver qu'une seule copie dans StorageGRID et envoyer une copie au pool de stockage cloud.	Le service de réplication CloudMirror permet à un locataire de répliquer automatiquement les objets depuis 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.
Comment est-il configuré ?	Les pools de stockage cloud sont définis de la même manière que les pools de stockage, à l'aide de Grid Manager ou de l'API de gestion du grid. Un pool de stockage cloud peut être sélectionné comme emplacement dans une règle ILM. Lorsqu'un pool de stockage est constitué d'un groupe de nœuds de stockage, un pool de stockage cloud est défini à l'aide d'un terminal S3 ou Azure distant (adresse IP, identifiants, etc.).	Un utilisateur locataire Configure la réplication CloudMirror En définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. Une fois le terminal CloudMirror configuré, tous les compartiments appartenant à ce compte peuvent être configurés pour pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	En général, un administrateur grid	Généralement, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Tier Azure Blob Archive	• Toute infrastructure S3 compatible (y compris Amazon S3)
Pourquoi déplacer des objets vers la destination ?	Une ou plusieurs règles ILM de la politique ILM active. Les règles ILM définissent le déplacement des objets StorageGRID vers le pool de stockage cloud et le déplacement des objets.	Le fait d'ingérer un nouvel objet dans un compartiment source qui a été configuré avec un nœud final CloudMirror. Les objets qui existaient dans le compartiment source avant que le compartiment n'ait été configuré avec le nœud final CloudMirror ne soient pas répliqués, à moins qu'ils ne soient 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 a également été supprimé dans le pool de stockage cloud.	L'action de suppression n'est pas répliquée. Un objet supprimé n'existe plus dans le compartiment StorageGRID, mais il continue d'exister dans le compartiment de destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.
Comment accéder aux objets après un incident (le système StorageGRID n'est pas opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Au cours de ce processus, les copies des objets répliqués peuvent être restaurées à l'aide de copies dans le pool de stockage cloud.	Les copies d'objets de la destination CloudMirror sont indépendantes de StorageGRID, ce qui permet d'y accéder directement avant la restauration des nœuds StorageGRID.

Création d'un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud, vous indiquez le nom et l'emplacement du compartiment ou du conteneur externe utilisé par StorageGRID pour stocker des objets, le type de fournisseur cloud (Amazon S3 ou Azure Blob Storage) et le StorageGRID service d'information doit accéder au compartiment ou au conteneur externe.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez lu les instructions de configuration des pools de stockage cloud.
- Le compartiment ou conteneur externe référencé par le pool de stockage cloud existe déjà.
- Vous disposez de toutes les informations d'authentification requises pour accéder au compartiment ou au conteneur.

Description de la tâche

Un pool de stockage cloud spécifie un compartiment S3 externe unique ou un conteneur de stockage Azure Blob. 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.

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche. Cette page contient deux sections : les pools de stockage et les pools de stockage cloud.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit Remove View Details

Name ?	Used Space ?	Free Space ?	Total Capacity ?	ILM Usage ?
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit Remove Clear Error

No Cloud Storage Pools found.

2. Dans la section Cloud Storage pools de la page, sélectionnez **Create**.

La boîte de dialogue Créer un pool de stockage cloud s'affiche.

Create Cloud Storage Pool

Display Name ?

Provider Type ?

Bucket or Container ?

Cancel

Save

3. Saisissez les informations suivantes :

Champ	Description
Afficher le nom	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 : sélectionnez cette option pour un terminal S3, C2S S3 ou Google Cloud Platform (GCP). • Stockage Azure Blob Remarque : lorsque vous sélectionnez un type de fournisseur, les sections point de terminaison de service, authentification et vérification du serveur s'affichent en bas de la page.
Godet ou conteneur	Nom du compartiment S3 externe ou du conteneur Azure créé pour le pool de stockage cloud. Le nom que vous indiquez ici doit correspondre exactement au nom du compartiment ou du conteneur, ou la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l'enregistrement du pool de stockage cloud.

4. Complétez les sections point de terminaison de service, authentification et vérification du serveur de la page, en fonction du type de fournisseur sélectionné.

- [S3 : spécifiez les détails d'authentification pour un pool de stockage cloud](#)
- [C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud](#)
- [Azure : spécifiez les détails d'authentification pour un pool de stockage cloud](#)

S3 : spécification des détails d'authentification pour un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud pour S3, vous devez sélectionner le type d'authentification requis pour le terminal Cloud Storage Pool. Vous pouvez spécifier Anonyme ou entrer un ID de clé d'accès et une clé d'accès secrète.

Ce dont vous avez besoin

- Vous avez saisi les informations de base pour le pool de stockage cloud et spécifié **Amazon S3** comme type de fournisseur.

Create Cloud Storage Pool

Display Name ?

S3 Cloud Storage Pool

Provider Type ?

Amazon S3 ▼

Bucket or Container ?

my-s3-bucket

Service Endpoint

Protocol ?

☐ HTTP ☒ HTTPS

Hostname ?

example.com or 0.0.0.0

Port (optional) ?

443

URL Style ?

Auto-Detect ▼

Authentication

Authentication Type ?

▼

Server Verification

Certificate Validation ?

Use operating system CA certificate ▼

Cancel

Save

- Si vous utilisez l'authentification par clé d'accès, vous connaissez l'ID de clé d'accès et la clé d'accès

secrète pour le compartiment S3 externe.

Étapes

1. Dans la section **Service Endpoint**, fournissez les informations suivantes :

a. Sélectionnez le protocole à utiliser lors de la connexion au pool de stockage cloud.

Le protocole par défaut est HTTPS.

b. Entrez le nom d'hôte ou l'adresse IP du serveur du pool de stockage cloud.

Par exemple :

`s3-aws-region.amazonaws.com`



Ne pas inclure le nom de compartiment dans ce champ. Vous incluez le nom du compartiment dans le champ **godet ou conteneur**.

a. Spécifiez éventuellement le port à utiliser lors de la connexion au Cloud Storage Pool.

Laissez ce champ vide pour utiliser le port par défaut : port 443 pour HTTPS ou port 80 pour HTTP.

b. Sélectionnez le style d'URL du compartiment de pool de stockage cloud :

Option	Description
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, par 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 style chemin d'accès incluent le nom du compartiment à la fin, par exemple <code>https://s3.company.com/bucket-name/key-name</code> . Note: l'URL de style de chemin d'accès est obsolète.
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.

2. Dans la section **Authentication**, sélectionnez le type d'authentification requis pour le terminal Cloud Storage Pool.

Option	Description
Clé d'accès	Un ID de clé d'accès et une clé d'accès secrète sont nécessaires pour accéder au compartiment de pool de stockage cloud.

Option	Description
Anonyme	Tout le monde a accès au compartiment Cloud Storage Pool. Un ID de clé d'accès et une clé d'accès secrète ne sont pas nécessaires.
CAP (portail d'accès C2S)	Utilisé uniquement pour C2S S3. Accédez à C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud .

3. Si vous avez sélectionné clé d'accès, saisissez les informations suivantes :

Option	Description
ID de clé d'accès	ID de clé d'accès du compte propriétaire du compartiment externe.
Clé d'accès secrète	La clé d'accès secrète associée.

4. Dans la section Server Verification, sélectionnez la méthode à utiliser pour valider le certificat pour les connexions TLS au Cloud Storage Pool :

Option	Description
Utiliser le certificat CA du système d'exploitation	Utilisez les certificats d'autorité de certification de la grille installés par défaut 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 Sélectionner nouveau et téléchargez le certificat d'autorité de certification codé PEM.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié.

5. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide la présence du compartiment et du point de terminaison de service et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.
- Écrit un fichier de marqueur dans le compartiment pour identifier le compartiment comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment spécifié n'existe pas déjà.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Reportez-vous aux instructions pour [Résolution des problèmes avec les pools de stockage cloud](#), Réglez le problème, puis réessayez d'enregistrer le pool de stockage cloud.

C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud

Pour utiliser le service S3 commercial Cloud Services (C2S) comme pool de stockage cloud, vous devez configurer C2S Access Portal (CAP) comme type d'authentification. StorageGRID peut ainsi demander des identifiants temporaires pour accéder au compartiment S3 de votre compte C2S.

Ce dont vous avez besoin

- Vous avez saisi les informations de base d'un pool de stockage cloud Amazon S3, y compris le terminal du service.
- Vous connaissez l'URL complète utilisée par StorageGRID pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API obligatoires et facultatifs attribués à votre compte C2S.
- Vous disposez d'un certificat d'autorité de certification de serveur délivré par une autorité de certification du gouvernement (AC) appropriée. StorageGRID utilise ce certificat pour vérifier l'identité du serveur CAP. Le certificat d'autorité de certification du serveur doit utiliser le codage PEM.
- Vous avez un certificat de client émis par une autorité de certification gouvernementale (AC) appropriée. StorageGRID utilise ce certificat pour s'identifier lui-même au serveur CAP. Le certificat client doit utiliser le codage PEM et avoir reçu l'accès à votre compte C2S.
- Vous disposez d'une clé privée codée PEM pour le certificat client.
- Si la clé privée du certificat client est cryptée, vous disposez de la phrase de passe pour le déchiffrer.

Étapes

1. Dans la section **authentification**, sélectionnez **CAP (portail d'accès C2S)** dans la liste déroulante **Type d'authentification**.

Les champs d'authentification CAP C2S s'affichent.

Create Cloud Storage Pool

Display Name  C2S Cloud Storage Pool

Provider Type  Amazon S3 ▼

Bucket or Container  my-c2s-bucket

Service Endpoint

Protocol  ☐ HTTP ☒ HTTPS

Hostname  s3-aws-region.amazonaws.com

Port (optional)  443

URL Style  Auto-Detect ▼

Authentication

Authentication Type  CAP (C2S Access Portal) ▼

Temporary Credentials URL  https://example.com/CAP/api/v1/cred

Server CA Certificate  [Select New](#)

Client Certificate  [Select New](#)

Client Private Key  [Select New](#)

Client Private Key
Passphrase (optional) 

Server Verification

Certificate Validation  Use operating system CA certificate ▼

Cancel

Save

2. Fournissez les informations suivantes :

- a. Pour **URL d'informations d'identification temporaires**, entrez l'URL complète utilisée par StorageGRID pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API obligatoires et facultatifs attribués à votre compte C2S.
- b. Pour **certificat d'autorité de certification du serveur**, sélectionnez **Sélectionner nouveau** et téléchargez le certificat d'autorité de certification codé au PEM que StorageGRID utilisera pour vérifier le serveur CAP.
- c. Pour **certificat client**, sélectionnez **Sélectionner nouveau** et téléchargez le certificat encodé au PEM que StorageGRID utilisera pour s'identifier au serveur CAP.
- d. Pour **clé privée client**, sélectionnez **Sélectionner nouveau** et téléchargez la clé privée codée PEM pour le certificat client.

Si la clé privée est cryptée, le format traditionnel doit être utilisé. (Le format crypté PKCS #8 n'est pas pris en charge.)

- 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 **Mot de passe de clé privée client** vide.

3. Dans la section Vérification du serveur, fournissez les informations suivantes :

- a. Pour **validation de certificat**, sélectionnez **utiliser le certificat d'autorité de certification personnalisé**.
- b. Sélectionnez **Sélectionner nouveau** et téléchargez le certificat d'autorité de certification codé PEM.

4. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide la présence du compartiment et du point de terminaison de service et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.
- Écrit un fichier de marqueur dans le compartiment pour identifier le compartiment comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment spécifié n'existe pas déjà.

Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Reportez-vous aux instructions pour [Résolution des problèmes avec les pools de stockage cloud](#), Résolvez le problème, puis réessayez d'enregistrer le pool de stockage cloud.

Azure : spécifiez les détails d'authentification pour un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud pour le stockage Azure Blob, vous devez spécifier un nom de compte et une clé de compte pour le conteneur externe que StorageGRID utilisera pour stocker des objets.

Ce dont vous avez besoin

- Vous avez saisi les informations de base pour le pool de stockage cloud et spécifié **Azure Blob Storage** comme type de fournisseur. **Clé partagée** apparaît dans le champ **Type d'authentification**.

Create Cloud Storage Pool

Display Name ⓘ

Azure Cloud Storage Pool

Provider Type ⓘ

Azure Blob Storage ▼

Bucket or Container ⓘ

my-azure-container

Service Endpoint

URI ⓘ

https://myaccount.blob.core.windows.net

Authentication

Authentication Type ⓘ

Shared Key

Account Name ⓘ

Account Key ⓘ

Server Verification

Certificate Validation ⓘ

Use operating system CA certificate ▼

Cancel

Save

- L'URI (Uniform Resource identifier) utilisé pour accéder au conteneur de stockage Blob utilisé pour le pool de stockage cloud.
- Vous connaissez le nom du compte de stockage et la clé secrète. Utilisez le portail Azure pour trouver ces

valeurs.

Étapes

1. Dans la section **Service Endpoint**, entrez l'URI (Uniform Resource identifier) utilisé pour accéder au conteneur de stockage Blob utilisé pour le pool de stockage cloud.

Spécifiez l'URI dans l'un des formats suivants :

- `https://host:port`
- `http://host:port`

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour les URI HTTPS et le port 80 est utilisé pour les URI HTTP. + **exemple d'URI pour conteneur de stockage Azure Blob** :

`https://myaccount.blob.core.windows.net`

2. Dans la section **authentification**, fournissez les informations suivantes :

- a. Pour **Nom de compte**, entrez le nom du compte de stockage Blob qui possède le conteneur de services externes.
- b. Pour **clé de compte**, saisissez la clé secrète du compte de stockage Blob.



Pour les terminaux Azure, vous devez utiliser l'authentification Shared Key.

3. Dans la section **Vérification du serveur**, sélectionnez la méthode à utiliser pour valider le certificat pour les connexions TLS au pool de stockage cloud :

Option	Description
Utiliser le certificat CA du système d'exploitation	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 Sélectionner nouveau et téléchargez le certificat codé PEM.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié.

4. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide que le conteneur et l'URI existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
- Écrit un fichier de marqueur vers le conteneur pour l'identifier comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée s'il y a une erreur de certificat ou si le conteneur spécifié n'existe pas déjà.

Reportez-vous aux instructions pour [Résolution des problèmes avec les pools de stockage cloud](#), Résolvez le problème, puis réessayez d'enregistrer le pool de stockage cloud.

Modifiez un pool de stockage cloud

Vous pouvez modifier un pool de stockage cloud pour en changer le nom, le terminal de service ou d'autres détails. Toutefois, vous ne pouvez pas modifier le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue le [Considérations relatives aux pools de stockage cloud](#).

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche. Le tableau Cloud Storage pools répertorie les pools de stockage cloud existants.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create	✎ Edit	✕ Remove	Clear Error			
	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
☒	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
☐	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	
Displaying 2 pools.						

2. Sélectionnez le bouton radio correspondant au pool de stockage cloud que vous souhaitez modifier.
3. Sélectionnez **Modifier**.
4. Si nécessaire, modifiez le nom d'affichage, le point de terminaison de service, les informations d'identification d'authentification ou la méthode de validation de certificat.



Vous ne pouvez pas modifier le type de fournisseur, le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Si vous avez déjà téléchargé un certificat de serveur ou de client, vous pouvez sélectionner **Afficher actuel** pour vérifier le certificat actuellement utilisé.

5. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID valide la présence du compartiment ou du conteneur et du terminal de service, et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche. Par exemple, une erreur peut être signalée en cas d'erreur de certificat.

Reportez-vous aux instructions pour [Résolution des problèmes avec les pools de stockage cloud](#), Réglez le problème, puis réessayez d'enregistrer le pool de stockage cloud.

Supprimez un pool de stockage cloud

Vous pouvez supprimer un pool de stockage cloud qui n'est pas utilisé dans une règle ILM et qui ne contient pas de données d'objet.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez 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`.

- Vous avez déjà supprimé toutes les règles ILM susceptibles d'avoir utilisé le pool.

Étapes

1. Sélectionnez **ILM Storage pools**.

La page Storage pools s'affiche.

2. Sélectionnez le bouton radio d'un pool de stockage cloud qui n'est pas actuellement utilisé dans une règle ILM.

Vous ne pouvez pas supprimer un pool de stockage cloud s'il est utilisé dans une règle ILM. Le bouton **Supprimer** est désactivé.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit ✕ Remove Clear Error						
	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
☒	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
☐	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	

Displaying 2 pools.

3. Sélectionnez **Supprimer**.

Un avertissement de confirmation s'affiche.

⚠ Warning

Remove Cloud Storage Pool

Are you sure you want to remove this Cloud Storage Pool: My Cloud Storage Pool?

Cancel

OK

4. Sélectionnez **OK**.

Le pool de stockage cloud est supprimé.

Résoudre les problèmes liés aux pools de stockage cloud

Si vous rencontrez des erreurs lors de la création, de la modification ou de la suppression d'un pool de stockage cloud, utilisez ces étapes de dépannage pour résoudre le problème.

Déterminez si une erreur s'est produite

StorageGRID effectue une vérification simple de l'état de santé de chaque pool de stockage cloud une fois par minute pour vérifier que celui-ci est accessible et qu'il fonctionne correctement. Si le contrôle de l'état de santé détecte un problème, un message s'affiche dans la colonne dernière erreur du tableau Cloud Storage pools sur la page Storage pools.

Le tableau indique la dernière erreur détectée pour chaque pool de stockage cloud et indique la durée de l'erreur.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit ✖ Remove Clear Error					
Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
☒ S3	10.96.106.142:18082	s3	s3	✓	Endpoint failure: DC2-S1-106-147: Could not create or update Cloud Storage Pool. Error from endpoint: RequestError: send request failed caused by: Get https://10.96.106.142:18082/s3-targetbucket/x-ntap-sgws-cloud-pool-uuid: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers) 8 minutes ago
☐ Azure	http://pboerkoe@10.96.100.254:10000/d-evstoreaccount1	azure	azure	✓	

Displaying 2 pools.

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 Pool (sélectionnez **ILM Storage pools**), examinez 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 bouton radio du noeud final et sélectionnez **Effacer erreur**. Un message

de confirmation indique que StorageGRID a résolu l'erreur pour le pool de stockage cloud.

Error successfully cleared. This error might reappear if the underlying problem is not resolved.



Si le problème sous-jacent a été résolu, le message d'erreur ne s'affiche plus. Cependant, 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 quelques minutes.

Erreur : ce pool de stockage cloud contient du contenu inattendu

Cette erreur peut se produire lorsque vous tentez de créer, modifier ou supprimer un pool de stockage cloud. Cette erreur se produit si le godet ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid`. Le fichier de marqueurs, mais ce fichier n'a pas l'UUID attendu.

En général, cette erreur s'affiche uniquement si vous créez un pool de stockage cloud et qu'une autre instance de StorageGRID utilise déjà le même pool de stockage cloud.

Essayez ces étapes pour corriger le problème :

- Assurez-vous que personne dans votre entreprise n'utilise également ce Cloud Storage Pool.
- Supprimez le `x-ntap-sgws-cloud-pool-uuid`. Et essayez à nouveau de configurer le pool de stockage cloud.

Erreur : impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID d'écrire dans le pool de stockage cloud.

Pour corriger le problème, consultez le message d'erreur du noeud final.

- Si le message d'erreur contient `Get url: EOF`, Vérifiez que le point de terminaison de service utilisé pour Cloud Storage Pool n'utilise pas le protocole HTTP pour un conteneur ou un compartiment qui nécessite HTTPS.
- Si le message d'erreur contient `Get url: net/http: request canceled while waiting for connection`, Vérifiez que la configuration réseau autorise les nœuds de stockage à accéder au terminal de service utilisé pour le pool de stockage cloud.
- Pour tous les autres messages d'erreur de point final, essayez un ou plusieurs des éléments suivants :
 - Créez un conteneur ou un compartiment externe avec le même nom que vous avez saisi pour le Cloud Storage Pool, et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
 - Corrigez le nom de conteneur ou de compartiment que vous avez spécifié pour le pool de stockage cloud, et essayez de sauvegarder à nouveau le nouveau pool de stockage cloud.

Erreur : échec de l'analyse du certificat CA

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. L'erreur se produit si StorageGRID n'a pas pu analyser le certificat que vous avez saisi lors de la configuration du pool de stockage cloud.

Pour corriger le problème, vérifiez si le certificat CA que vous avez fourni ne présente pas de problèmes.

Erreur : un pool de stockage cloud associé à cet ID est introuvable

Cette erreur peut se produire lorsque vous essayez de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le noeud final renvoie une réponse 404, ce qui peut signifier l'un des éléments suivants :

- Les identifiants utilisés pour Cloud Storage Pool ne disposent pas d'une autorisation de lecture pour le compartiment.
- Le compartiment utilisé pour le pool de stockage cloud n'inclut pas la `x-ntap-sgws-cloud-pool-uuid` fichier de marqueur.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée possède les autorisations requises.
- Modifiez le pool de stockage cloud avec des identifiants disposant des autorisations requises.
- Si les autorisations sont correctes, contactez l'assistance technique.

Erreur : impossible de vérifier le contenu du pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID de lire le contenu du compartiment Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur du noeud final.

Erreur : les objets ont déjà été placés dans ce compartiment

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Vous ne pouvez pas supprimer un pool de stockage cloud si celui-ci contient des données déplacées par ILM, celles qui se trouvent dans le compartiment avant de configurer le pool de stockage cloud, ou celles 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 survient si le serveur proxy externe ne peut pas atteindre le terminal Cloud Storage Pool. Par exemple, il se peut que le serveur DNS ne puisse pas résoudre le nom d'hôte ou qu'il existe un problème de réseau externe.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez les paramètres de Cloud Storage Pool (**ILM Storage pools**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Informations associées

[Cycle de vie d'un objet de pool de stockage cloud](#)

Configurez les profils de code d'effacement

Créez un profil de code d'effacement

Pour créer un profil de code d'effacement, vous associez un pool de stockage contenant des nœuds de stockage à un schéma de code d'effacement. Cette association détermine le nombre de données et de fragments de parité créés et l'endroit où le système distribue ces fragments.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez créé un pool de stockage qui comprend exactement un site ou un pool de stockage comprenant trois sites ou plus. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage possédant que deux sites seulement.

Description de la tâche

Les pools de stockage utilisés dans les profils de code d'effacement doivent inclure exactement un ou trois sites ou plus. Si vous souhaitez fournir une redondance de site, le pool de stockage doit avoir au moins trois sites.



Vous devez sélectionner un pool de stockage contenant des nœuds de stockage. Vous ne pouvez pas utiliser les nœuds d'archivage pour les données avec code d'effacement.

Étapes

1. Sélectionnez **ILM codage d'effacement**.

La page profils de code d'effacement s'affiche.

Erasure Coding Profiles ⓘ

An Erasure Coding profile determines how many data and parity fragments are created and where those fragments are stored.

To create an Erasure Coding profile, select a [storage pool](#) and an erasure coding scheme. The storage pool must include Storage Nodes from exactly one site or from three or more sites. If you want to provide site redundancy, the storage pool must include nodes from at least three sites.

To deactivate an Erasure Coding profile that you no longer plan to use, first remove it from all ILM rules. Then, if the profile is still associated with object data, wait for those objects to be moved to new locations based on the new rules in the active ILM policy. Depending on the number of objects and the size of your StorageGRID system, it might take weeks or even months for the objects to be moved.

See [Managing objects with information lifecycle management](#) for important details.

+ Create ✎ Rename ⛔ Deactivate									
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy	
No Erasure Coding profiles found.									

2. Sélectionnez **Créer**.

La boîte de dialogue Créer un profil EC s'affiche.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name 

Storage Pool 

Cancel

Save

3. Entrez un nom unique pour le profil de code d'effacement.

Les noms de profils de codage d'effacement doivent être uniques. Une erreur de validation se produit si vous utilisez le nom d'un profil existant, même si ce profil a été désactivé.



Le nom du profil d'effacement Coding est ajouté au nom du pool de stockage dans l'instruction de placement pour une règle ILM.

From day store Add Remove

Type Location Copies + x

Erasure Coding profile name

Storage pool name

4. Sélectionnez le pool de stockage que vous avez créé pour ce profil de code d'effacement.



Si votre grille ne contient actuellement qu'un seul site, vous ne pouvez pas utiliser le pool de stockage par défaut, tous les nœuds de stockage ou tout pool de stockage incluant le site par défaut, tous les sites. Ce comportement empêche le profil de code d'effacement de devenir non valide si un second site est ajouté.



Si un pool de stockage comprend exactement deux sites, vous ne pouvez pas utiliser ce pool de stockage pour le codage d'effacement. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage possédant deux sites.

Lorsque vous sélectionnez un pool de stockage, la liste des schémas de code d'effacement disponibles s'affiche, en fonction du nombre de nœuds de stockage et de sites du pool.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name  6 plus 3

Storage Pool  All 3 Sites 

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code 	Storage Overhead (%) 	Storage Node Redundancy 	Site Redundancy 
☒	6+3	50%	3	Yes
☐	2+1	50%	1	Yes
☐	4+2	50%	2	Yes

Cancel

Save

Pour chaque schéma de code d'effacement, les informations suivantes sont répertoriées :

- **Code d'effacement** : le nom du schéma de codage d'effacement dans le format suivant : fragments de données + fragments de parité.
- **Surcharge de stockage (%)** : stockage supplémentaire requis pour les fragments de parité par rapport à la taille des données de l'objet. Frais de stockage = nombre total de fragments de parité / nombre total de fragments de données.
- **Redondance de nœud de stockage** : nombre de nœuds de stockage qui peuvent être perdus tout en conservant la possibilité de récupérer des données d'objet.
- **Redondance de site** : si le code d'effacement sélectionné permet de récupérer les données d'objet en cas de perte d'un site.

Pour prendre en charge la redondance des sites, le pool de stockage sélectionné doit inclure plusieurs sites, chacun disposant de suffisamment de nœuds de stockage pour permettre la perte d'un site. Par exemple, pour prendre en charge la redondance de site à l'aide d'un schéma de code d'effacement 6+3, le pool de stockage sélectionné doit inclure au moins trois sites avec au moins trois nœuds de stockage sur chaque site.

Les messages s'affichent dans les cas suivants :

- Le pool de stockage que vous avez sélectionné ne fournit pas de redondance de site. Le message suivant est attendu lorsque le pool de stockage sélectionné ne comprend qu'un seul site. Vous pouvez utiliser ce profil de code d'effacement dans les règles ILM pour une protection contre les défaillances de nœuds.

Scheme

	Erasure Code 	Storage Overhead (%) 	Storage Node Redundancy 	Site Redundancy 
☒	2+1	50%	1	No

The selected storage pool and erasure coding scheme cannot protect object data from loss if a site is lost.
To provide site redundancy, the storage pool must have at least three sites.

- Le pool de stockage que vous avez sélectionné ne répond pas aux exigences d'un schéma de code d'effacement. Par exemple, le message suivant est attendu lorsque le pool de stockage sélectionné comprend exactement deux sites. Si vous souhaitez utiliser le code d'effacement pour protéger les données d'objet, vous devez sélectionner un pool de stockage avec exactement un site ou un pool de stockage avec trois sites ou plus.

Scheme

Erasure Code ?	Storage Overhead (%) ?	Storage Node Redundancy ?	Site Redundancy ?
No erasure coding schemes are supported for the selected storage pool because it contains two sites. You must select a storage pool that contains exactly one site or a storage pool that contains at least three sites.			

- Votre grille inclut un seul site et vous avez sélectionné le pool de stockage par défaut, tous les nœuds de stockage ou tout pool de stockage qui inclut le site par défaut, tous les sites.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool

3 Storage Nodes across 1 site(s)

Scheme

Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
No erasure coding schemes are available for the selected storage pool. The storage pool includes the All Sites site, so it cannot be used in an Erasure Coding profile for a one-site grid.			

Cancel

Save

- Le schéma de code d'effacement et le pool de stockage que vous avez sélectionnés se chevauchent avec un autre profil de code d'effacement.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name  2 plus 1 for three sites

Storage Pool  All 3 Sites

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code 	Storage Overhead (%) 	Storage Node Redundancy 	Site Redundancy 
☐	6+3	50%	3	Yes
☒	2+1	50%	1	Yes
☐	4+2	50%	2	Yes

The selected storage pool and erasure coding scheme overlap an existing Erasure Coding profile. Use caution if you apply this new profile to objects already protected by the other profile. When a new profile is applied to existing erasure-coded objects, entirely new erasure-coded fragments are created, which might cause resource issues.

Cancel

Save

Dans cet exemple, un message d'avertissement apparaît car un autre profil de code d'effacement utilise le schéma 2+1 et le pool de stockage de l'autre profil utilise également l'un des sites du pool de stockage des 3 sites.

Vous n'avez pas pu créer ce nouveau profil, mais il est très prudent de vous en servir dans la politique ILM. Si ce nouveau profil est appliqué aux objets avec code d'effacement déjà protégés par l'autre profil, StorageGRID crée un jeu entièrement nouveau de fragments d'objet. Il ne réutilise pas les fragments 2+1 existants. Des problèmes de ressources peuvent survenir lorsque vous migrez d'un profil de code d'effacement à l'autre, même si les schémas de code d'effacement sont les mêmes.

5. Si plusieurs codes d'effacement sont répertoriés, sélectionnez celui que vous souhaitez utiliser.

Lorsque vous décidez du schéma de code d'effacement à utiliser, vous devez équilibrer la tolérance aux pannes (obtenue en ayant plus de segments de parité) avec les exigences du trafic réseau pour les réparations (plus de fragments équivaut à davantage de trafic du réseau). Par exemple, lors du choix entre un schéma 4+2 et 6+3, sélectionnez le schéma 6+3 si une parité et une tolérance aux pannes supplémentaires sont requises. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées pour réduire l'utilisation du réseau lors des réparations de nœuds.

6. Sélectionnez **Enregistrer**.

Renommer un profil de code d'effacement

Vous pouvez renommer un profil de code d'effacement pour le rendre plus évident que le profil.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **ILM codage d'effacement**.

La page profils de code d'effacement s'affiche. Les boutons **Renommer** et **Désactiver** sont tous deux désactivés.

+ Create ✎ Rename ⊖ Deactivate									
	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
☐	DC1 2-1		DC1	3	1	2+1	50	1	No
☐	DC2 2-1		DC2	3	1	2+1	50	1	No
☐	DC3 2-1		DC3	3	1	2+1	50	1	No
☒	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Sélectionnez le profil à renommer.

Les boutons **Renommer** et **Désactiver** sont activés.

3. Sélectionnez **Renommer**.

La boîte de dialogue Renommer le profil EC s'affiche.

Rename EC Profile

Profile Name

Cancel Save

4. Entrez un nom unique pour le profil de code d'effacement.

Le nom du profil d'effacement Coding est ajouté au nom du pool de stockage dans l'instruction de placement pour une règle ILM.

From day store

Add Remove

Type

Location

Copies

+ x

Erasure Coding profile name

Storage pool name



Les noms de profils de codage d'effacement doivent être uniques. Une erreur de validation se produit si vous utilisez le nom d'un profil existant, même si ce profil a été désactivé.

5. Sélectionnez **Enregistrer**.

Désactivez un profil de code d'effacement

Vous pouvez désactiver un profil de code d'effacement si vous n'avez plus l'intention de l'utiliser et si le profil n'est pas actuellement utilisé dans les règles ILM.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez confirmé que aucune opération de réparation avec code d'effacement ou aucune procédure de désaffectation des données n'est en cours. Un message d'erreur s'affiche si vous tentez de désactiver un profil de code d'effacement alors que l'une de ces opérations est en cours.

Description de la tâche

Lorsque vous désactivez un profil de code d'effacement, le profil apparaît toujours sur la page profils de code d'effacement, mais son état est **désactivé**.

+ Create Rename Deactivate									
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy	
☐ DC1 2-1		DC1	3	1	2+1	50	1	No	
☐ DC2 2-1		DC2	3	1	2+1	50	1	No	
☐ DC3 2-1		DC3	3	1	2+1	50	1	No	
☒ All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes	

Vous ne pouvez plus utiliser un profil de code d'effacement qui a été désactivé. Un profil désactivé n'apparaît pas lorsque vous créez les instructions de placement pour une règle ILM. Vous ne pouvez pas réactiver un profil désactivé.

StorageGRID vous empêche de désactiver un profil de code d'effacement si l'un des éléments suivants est vrai :

- 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 d'objet et les fragments de parité pour le profil existent toujours.

Étapes

1. Sélectionnez **ILM codage d'effacement**.

La page profils de code d'effacement s'affiche. Les boutons **Renommer** et **Désactiver** sont tous deux désactivés.

2. Consultez la colonne **Status** pour confirmer que le profil de codage d'effacement que vous souhaitez désactiver n'est pas utilisé dans les règles ILM.

Vous ne pouvez pas désactiver un profil de code d'effacement s'il est utilisé dans une règle ILM. Dans l'exemple, le profil EC **2_1** est utilisé dans au moins une règle ILM.

+ Create Rename Deactivate									
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy	
☐ 2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No	
☐ Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No	

3. Si le profil est utilisé dans une règle ILM, effectuez la procédure suivante :

- Sélectionnez **ILM règles**.
- Pour chaque règle répertoriée, sélectionnez le bouton radio et consultez le diagramme de rétention pour déterminer si la règle utilise le profil de code d'effacement que vous souhaitez désactiver.

Dans l'exemple, la règle **Three site EC for plus grands objets** utilise un pool de stockage appelé **all 3 sites** et le profil de codage d'effacement **all sites 6-3**. Les profils de codage d'effacement sont représentés par cette icône : 

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

+ Create

Clone

Edit

Remove

Name	Used In Active Policy	Used In Proposed Policy
2 copy replication for smaller objects		
Three site EC for larger objects	✓	
Make 2 Copies		

Three site EC for larger objects

Description:

6-3 erasure coding at 3 sites for objects larger than 200 KB

Ingest Behavior:

Balanced

Reference Time:

Ingest Time

Filtering Criteria:

Matches all of the following metadata:

System Metadata

Object Size (MB)

greater than

0.2

Retention Diagram:

Trigger

Day 0

Duration

Forever

All 3 Sites (All sites 6-3)

- a. Si la règle ILM utilise le profil de code d'effacement que vous souhaitez désactiver, déterminez si la règle est utilisée soit dans la politique ILM active, soit dans une règle proposée.

Dans l'exemple, la règle EC **Three site pour les objets plus volumineux** est utilisée dans la politique ILM active.

- b. Suivez les étapes supplémentaires du tableau, en fonction de l'emplacement 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 codage d'effacement. ii. Poursuivre cette procédure.	Utilisation des règles ILM et des règles ILM

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
Règle ILM faisant actuellement partie de la politique ILM active	i. Cloner la règle active. ii. Supprimez la règle ILM qui utilise 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. Vous pouvez tenter en toute sécurité de désactiver un profil de code d'effacement alors qu'il est toujours associé aux données, mais 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 codage d'effacement. vii. Poursuivre cette procédure.	• Création d'une règle ILM • Utilisation des règles ILM et des règles ILM

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
La règle ILM faisant actuellement partie d'une politique ILM proposée	i. Modifier la règle proposée. ii. Supprimez la règle ILM qui utilise le profil de code d'effacement. iii. Ajoutez une ou plusieurs nouvelles règles ILM pour protéger tous les objets. iv. Enregistrez la stratégie proposée. v. Modifiez ou supprimez la règle que vous avez supprimée de la stratégie. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de codage d'effacement. vi. Poursuivre cette procédure.	• Création d'une règle ILM • Utilisation des règles ILM et des règles ILM
La règle ILM d'une règle ILM historique	i. Modifiez ou supprimez la règle. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de codage d'effacement. (La règle apparaît désormais comme une règle historique dans la politique historique.) ii. Poursuivre cette procédure.	Utilisation des règles ILM et des règles ILM

c. Actualisez la page profils de code d'effacement pour vous assurer que le profil n'est pas utilisé dans une règle ILM.

4. Si le profil n'est pas utilisé dans une règle ILM, sélectionnez le bouton radio et sélectionnez **Désactiver**.

La boîte de dialogue Désactiver le profil EC s'affiche.

Deactivate EC Profile

Are you sure you want to deactivate the profile 'All sites 6-3'?

StorageGRID will confirm that the profile is safe to remove (not used in any ILM rules and no longer associated with any object data). After this profile is deactivated, you can no longer use it.

Cancel
Deactivate

5. Si vous êtes sûr de vouloir désactiver le profil, sélectionnez **Désactiver**.

- Si StorageGRID est capable de désactiver le profil de codage d'effacement, son état est **désactivé**. Vous ne pouvez plus sélectionner ce profil pour une règle ILM.
- Si StorageGRID ne peut pas désactiver le profil, un message d'erreur s'affiche. Par exemple, un message d'erreur s'affiche si les données d'objet sont toujours associées à ce profil. Vous devrez peut-

être attendre plusieurs semaines avant d'essayer à nouveau le processus de désactivation.

Configuration des régions (facultatif et S3 uniquement)

Les règles ILM permettent de filtrer des objets en fonction des régions où des compartiments S3 sont créés, ce qui vous permet de stocker des objets provenant de différentes régions dans différents emplacements de stockage. Si vous souhaitez utiliser une région de compartiment S3 comme filtre dans une règle, vous devez d'abord créer les régions à utiliser par les compartiments du système.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque vous créez un compartiment S3, vous pouvez spécifier une région. La spécification d'une région permet au compartiment d'être géographiquement proche de ses utilisateurs, ce qui peut contribuer à optimiser la latence, réduire les coûts et satisfaire aux exigences réglementaires.

Lorsque vous créez une règle ILM, vous pouvez utiliser la région associée à un compartiment S3 comme filtre avancé. Par exemple, vous pouvez concevoir une règle qui s'applique uniquement aux objets des compartiments S3 créés dans la région US-West-2. Afin d'optimiser la latence, vous pouvez ensuite placer des copies de ces objets sur des nœuds de stockage sur un site de data Center dans cette région.

Lors de la configuration de régions, suivez les consignes suivantes :

- Par défaut, tous les compartiments sont considérés comme appartenant à la région US-East-1.
- Vous devez créer les régions à l'aide de Grid Manager avant de spécifier une région autre que celle par défaut lors de la création de compartiments à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires ou avec l'élément de demande LocationConstraint pour les requêtes d'API PUT S3. Une erreur se produit si une demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.
- Lors de la création du compartiment S3, vous devez utiliser le nom exact de la région. Les noms de région sont sensibles à la casse et doivent comporter au moins 2 caractères et pas plus de 32 caractères. Les caractères autorisés sont des chiffres, des lettres et des tirets.



L'UE n'est pas considérée comme un alias pour l'ue-Ouest-1. Si vous souhaitez utiliser la région UE ou eu-West-1, vous devez utiliser le nom exact.

- Vous ne pouvez ni supprimer, ni modifier une région si elle est actuellement utilisée dans la politique ILM active ou la politique ILM proposée.
- Si la région utilisée comme filtre avancé dans une règle ILM n'est pas valide, il est toujours possible d'ajouter cette règle à la règle proposée. Cependant, une erreur se produit si vous tentez d'enregistrer ou d'activer la stratégie proposée. (Une région non valide peut se produire si vous utilisez une région comme filtre avancé dans une règle ILM mais que vous supprimez cette région ultérieurement, 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.

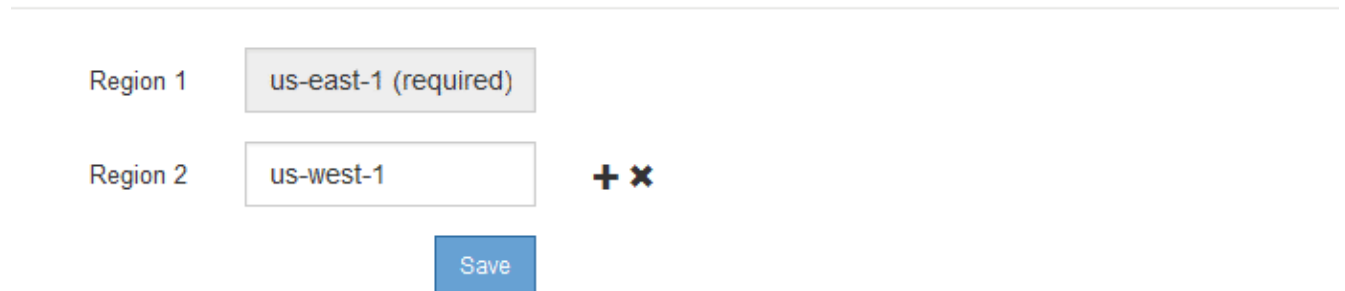
Étapes

1. Sélectionnez **ILM régions**.

La page régions s'affiche, les régions actuellement définies étant répertoriées. **Région 1** affiche la région par défaut, `us-east-1`, qui ne peut pas être modifié ou supprimé.

Regions (optional and S3 only)

Define any regions you want to use for the Location Constraint advanced filter in ILM rules. Then, use these exact names when creating S3 buckets. (Region names are case sensitive.)



Region 1

Region 2 + -

2. Pour ajouter une région :

- Sélectionnez l'icône Insérer **+** à droite de la dernière entrée.
- Entrez le nom d'une région à utiliser lors de la création de compartiments S3.

Vous devez utiliser ce nom de région exact comme élément de demande `LocationConstraint` lorsque vous créez le compartiment S3 correspondant.

3. Pour supprimer une région inutilisée, sélectionnez l'icône de suppression **-**.

Un message d'erreur s'affiche si vous tentez de supprimer une région actuellement utilisée dans la stratégie active ou la stratégie proposée.

 **Error**

422: Unprocessable Entity

Regions cannot be deleted if they are used by the active or the proposed ILM policy. In use:
`us-test-3`.

4. Une fois les modifications effectuées, sélectionnez **Enregistrer**.

Vous pouvez maintenant sélectionner ces régions dans la liste **contrainte d'emplacement** de la page filtrage avancé de l'assistant de création de règles ILM. Voir [Utilisation de filtres avancés dans les règles ILM](#).

Création d'une règle ILM

Accédez à l'assistant de création de règle ILM

Les règles ILM permettent de gérer le placement des données d'objet au fil du temps. Pour créer une règle ILM, utilisez l'assistant de création de règle ILM.



Si vous créez la règle ILM par défaut d'une règle, utilisez la procédure suivante : [Créez une règle ILM par défaut](#).

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Si vous souhaitez spécifier les comptes de tenant auxquels cette règle s'applique, vous disposez de l'autorisation comptes de tenant ou vous connaissez l'ID de compte de chaque compte.
- Pour que la règle filtre les objets sur les métadonnées de l'heure du dernier accès, les mises à jour de l'heure du dernier accès doivent être activées par compartiment pour S3 ou par conteneur pour Swift.
- Si vous créez des copies répliquées, vous avez configuré les pools de stockage ou les pools de stockage cloud que vous prévoyez d'utiliser. Voir [Créer un pool de stockage](#) et [Création d'un pool de stockage cloud](#).
- Si vous créez des copies avec code d'effacement, vous avez configuré un profil de code d'effacement. Voir [Créez un profil de code d'effacement](#).
- Vous connaissez le [options de protection des données pour l'ingestion](#).
- Si vous devez créer une règle compatible pour une utilisation avec le verrouillage d'objet S3, vous connaissez le [Conditions requises pour le verrouillage d'objet S3](#).
- Vous pouvez également regarder la vidéo : "[Vidéo : règles ILM de StorageGRID : mise en route](#)".



Description de la tâche

Lors de la création de règles ILM :

- Comparez la topologie et les configurations de stockage du système StorageGRID.
- Déterminez les types de copies d'objet à effectuer (répliquées ou avec code d'effacement) et le nombre de copies de chaque objet requis.
- Déterminez les types de métadonnées d'objet utilisés dans les applications qui se connectent au système StorageGRID. Les règles ILM filtrent les objets en fonction de leurs métadonnées.

- Réfléchissez à l'emplacement souhaité pour le stockage des copies d'objets au fil du temps.
- Choisissez l'option de protection des données à l'entrée des données (équilibrée, stricte ou double allocation).

Étapes

1. Sélectionnez **ILM règles**.

La page règles ILM apparaît, avec la règle de stock, faire 2 copies, sélectionnée.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

+

 Create

📄

 Clone

✎

 Edit

✖

 Remove

Name	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	

Make 2 Copies

Ingest Behavior:

Dual commit

Reference Time:

Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:

Trigger

Day 0

All Storage Nodes

Duration

Forever



La page règles ILM diffère légèrement si le paramètre global de verrouillage d'objet S3 a été activé pour le système StorageGRID. Le tableau récapitulatif comprend une colonne **compatible** et les détails de la règle sélectionnée incluent un champ **compatible**.

2. Sélectionnez **Créer**.

L'étape 1 (définir les bases) de l'assistant Créer une règle ILM s'affiche. La page définir les bases permet de définir les objets auxquels la règle s'applique.

Étape 1 sur 3 : définir les bases

L'étape 1 (Define Basics) de l'assistant Create ILM Rule (Créer une règle ILM) vous permet de définir les filtres de base et avancés de la règle.

Description de la tâche

Lors de l'évaluation d'un objet par rapport à une règle ILM, StorageGRID compare les métadonnées d'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.

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Étapes

1. Entrez un nom unique pour la règle dans le champ **Nom**.

Vous devez entrer entre 1 et 64 caractères.

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.

Name

Description

3. Vous pouvez également sélectionner un ou plusieurs comptes de locataires S3 ou Swift auxquels s'applique cette règle. Si cette règle s'applique à tous les locataires, laissez ce champ vide.

Si vous ne disposez pas des droits d'accès racine ou aux comptes de tenant, vous ne pouvez pas sélectionner de locataires dans la liste. Entrez plutôt l'ID de tenant ou entrez plusieurs ID comme une chaîne délimitée par des virgules.

4. Vous pouvez également spécifier les compartiments S3 ou les conteneurs Swift auxquels s'applique cette règle.

Si **correspond à tout** est sélectionné (par défaut), la règle s'applique à tous les compartiments S3 ou conteneurs Swift.

5. Vous pouvez également sélectionner **filtre avancé** pour spécifier des filtres supplémentaires.

Si vous ne configurez pas le filtrage avancé, la règle s'applique à tous les objets qui correspondent aux filtres de base.

Si cette règle crée des copies avec code d'effacement, ajoutez le filtre avancé **Object Size (MB)** et définissez-le sur **supérieur à 1**. Le filtre de taille garantit que les objets de 1 Mo ou plus petits ne sont pas codés d'effacement.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement.

6. Sélectionnez **Suivant**.

L'étape 2 (définir les Placements) s'affiche.

Informations associées

- [Définition d'une règle ILM](#)
- [Utilisation de filtres avancés dans les règles ILM](#)
- [Étape 2 sur 3 : définir les placements](#)

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 de récupération (microsecondes)	• égal à • n'est pas égal • inférieur à • inférieur ou égal à • supérieur à • supérieur ou égal à	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 de temps d'incorporation dans n'importe quelle règle qui pourrait modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps de transfert sur une valeur supérieure ou égale à la durée approximative de mise en œuvre de la nouvelle stratégie pour garantir que les objets existants ne sont pas déplacés inutilement.
Clé	• égal à • n'est pas égal • contient • ne contient pas • commence par • ne commence pas par • se termine par • ne se termine pas par	Une clé d'objet S3 ou Swift unique ou complète le système. Par exemple, vous pouvez faire correspondre les objets qui se terminent avec <code>.txt</code> ou commencez par <code>test-object/</code> .

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Heure du dernier accès (microsecondes)	• égal à • n'est pas égal • inférieur à • inférieur ou égal à • supérieur à • supérieur ou égal à • existe • n'existe pas	Heure et date de la dernière récupération de l'objet (lecture ou visualisation). Remarque : si vous prévoyez d'utiliser l'heure du dernier accès comme filtre avancé, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3 ou le conteneur Swift. Utiliser l'heure du dernier accès dans les règles ILM
Contrainte d'emplacement (S3 uniquement)	• égal à • n'est pas égal	Région dans laquelle un compartiment S3 a été créé. Utilisez ILM régions pour définir les régions affichées. Note: Une valeur US-est-1 fera correspondre des objets dans des compartiments créés dans la région US-est-1 ainsi que des objets dans des compartiments n'ayant pas de région spécifiée. Configuration des régions (facultatif et S3 uniquement)
Taille de l'objet (Mo)	• égal à • n'est pas égal à • inférieur à • inférieur ou égal à • supérieur à • supérieur ou égal à	Taille de l'objet en Mo. Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement. Remarque : pour filtrer des tailles d'objet inférieures à 1 Mo, entrez une valeur décimale. Le type de navigateur et les paramètres régionaux contrôlent si vous devez utiliser un point ou une virgule comme séparateur décimal.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Métadonnées utilisateur	• contient • se termine par • égal à • existe • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par • commence par	Paire clé-valeur, où Nom de métadonnées utilisateur est la clé et valeur de métadonnées utilisateur la valeur. Par exemple, pour filtrer les objets dotés de métadonnées utilisateur de <code>color=blue</code>, spécifiez <code>color</code> Pour Nom de métadonnées utilisateur, <code>equals</code> pour l'opérateur, et <code>blue</code> Pour valeur de métadonnées utilisateur. Remarque : les noms de métadonnées utilisateur ne sont pas sensibles à la casse; les valeurs des métadonnées utilisateur sont sensibles à la casse.
Balise d'objet (S3 uniquement)	• contient • se termine par • égal à • existe • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par • commence par	Paire clé-valeur, où Nom de balise d'objet est la clé et valeur de balise d'objet la valeur. Par exemple, pour filtrer les objets qui ont une balise d'objet de <code>Image=True</code>, spécifiez <code>Image</code> Pour Nom de balise d'objet, <code>equals</code> pour l'opérateur, et <code>True</code> Pour valeur de balise d'objet. Remarque : les noms 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.

Spécification de 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 compris entre 10 Mo et 100 Mo, sélectionnez le type de métadonnées **Object Size** et spécifiez 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.

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Objects between 10 and 100 MB

Matches all of the following metadata:

Object Size (MB)	greater than or equals	10		
Object Size (MB)	less than or equals	100		
 				

Cancel

Remove Filters

Save

L'utilisation de plusieurs entrées vous permet d'avoir un contrôle précis sur les objets à associer. Dans l'exemple suivant, la règle s'applique aux objets dont la marque A ou la marque B est la valeur des métadonnées utilisateur Camera_type. Toutefois, la règle s'applique uniquement aux objets de marque B dont la taille est inférieure à 10 Mo.

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Multiple filters

Matches all of the following metadata:

User Metadata

camera_type

equals

Brand A

+

x

+

x

Or matches all of the following metadata:

User Metadata

camera_type

equals

Brand B

+

x

Object Size (MB)

less than or equals

10

+

x

+

x

Cancel

Remove Filters

Save

Étape 2 sur 3 : définir les placements

L'étape 2 (définir les Placements) de l'assistant de création de règles ILM permet de définir les instructions de placement qui déterminent la durée de stockage des objets, le type de copies (répliquées ou codées d'effacement), l'emplacement de stockage et le nombre de copies.

Description de la tâche

Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps. Lorsque vous utilisez plusieurs instructions, les périodes doivent être contiguës et au moins une instruction doit commencer le jour 0. Les instructions peuvent se poursuivre indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

Chaque instruction de placement peut avoir plusieurs lignes si vous voulez créer différents types de copies ou utiliser différents emplacements au cours de cette période.

Cet exemple de règle ILM crée deux copies répliquées pour la première année. Chaque copie est enregistrée dans un pool de stockage sur un site différent. Après un an, une copie avec code d'effacement pour 2+1 est effectuée et enregistrée sur un seul site.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Example rule
 Two copies for one year, then EC forever

Reference Time
 Ingest Time

Placements Sort by start day

From day 0 store for 365 days Add Remove

Type replicated Location DC1 DC2 Add Pool Copies 2 + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

From day 365 store forever Add Remove

Type erasure coded Location DC1 (2 plus 1) Copies 1 + x

Retention Diagram Refresh

Cancel Back Next

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 positionnement.

Option	Description
Temps d'ingestion	Heure à laquelle l'objet a été ingéré.
Heure du dernier accès	Heure à laquelle l'objet a été récupéré pour la dernière fois (lu ou affiché). Remarque : pour utiliser cette option, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3 ou le conteneur Swift. Voir Utiliser l'heure du dernier accès dans les règles ILM .

Option	Description
Heure non actuelle	Lorsqu'une version d'objet est devenue non actuelle car une nouvelle version a été ingérée et la remplace en tant que version actuelle. Remarque : le temps non courant s'applique uniquement aux objets S3 dans les compartiments avec gestion des versions. 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.
Heure de création définie par l'utilisateur	Heure spécifiée dans les métadonnées définies par l'utilisateur.



Si vous souhaitez créer une règle conforme, vous devez sélectionner **temps d'ingestion**.

2. Dans la section **Placements**, sélectionnez une heure de début et une durée pour la première période.

Par exemple, vous pouvez spécifier où stocker des objets pour la première année ("day 0 for 365 Days"). Au moins une instruction doit commencer au jour 0.

3. Pour créer des copies répliquées :

- a. Dans la liste déroulante **Type**, sélectionnez **Replicated**.
- b. Dans le champ **Location**, sélectionnez **Add Pool** pour chaque pool de stockage que vous souhaitez ajouter.

Si vous spécifiez un seul pool de stockage, sachez que StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si votre grid inclut trois nœuds de stockage et que vous sélectionnez 4 comme nombre de 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.

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. Pour cette raison, ne spécifiez pas le pool de stockage tous les nœuds de stockage par défaut et un autre pool de stockage.

Placements ⓘ ⇅ Sort by start day

From day store [Add](#) [Remove](#)

Type Location Copies + ×

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

c. Sélectionnez le nombre de copies à effectuer.

Un avertissement s'affiche si vous changez le nombre de copies en 1. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Voir [Pourquoi ne pas utiliser la réplication à copie unique](#).

Placements ⓘ ⇅ Sort by start day

From day store [Add](#) [Remove](#)

Type Location Copies Temporary location + ×

An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. [View additional details](#)

Pour éviter ces risques, effectuez l'une ou plusieurs des opérations suivantes :

- Augmentez le nombre de copies pour la période.
- Sélectionnez l'icône du signe plus **+** pour créer des copies supplémentaires pendant la période. Ensuite, sélectionnez un autre pool de stockage ou un pool de stockage cloud.
- Sélectionnez **code d'effacement** pour Type, au lieu de **répliqué**. Vous pouvez ignorer cet avertissement en toute sécurité si cette règle crée déjà plusieurs copies pour toutes les périodes.

d. Si vous n'avez spécifié qu'un seul pool de stockage, ignorez le champ **emplacement temporaire**.



Les emplacements temporaires sont obsolètes et seront supprimés dans une version ultérieure. Voir [Utiliser un pool de stockage comme emplacement temporaire \(obsolète\)](#).

4. Pour créer une copie avec code d'effacement :

a. Dans la liste déroulante **Type**, sélectionnez **code d'effacement**.

Le nombre de copies passe à 1. Un avertissement s'affiche si la règle n'a pas de filtre avancé pour ignorer les objets de 200 Ko ou moins.

Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to any value greater than 0.2.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement.

- b. Si l'avertissement de taille d'objet s'affiche, sélectionnez **Retour** pour revenir à l'étape 1. Sélectionnez ensuite **filtre avancé** et définissez le filtre taille d'objet (MB) sur une valeur supérieure à 0.2.
- c. Sélectionnez l'emplacement de stockage.

L'emplacement de stockage d'une copie avec code d'effacement inclut le nom du pool de stockage, suivi du nom du profil de code d'effacement.

From day 365 store forever Add Remove

Type erasure coded Location All 3 sites (6 plus 3) Copies 1 + x

Erasure Coding profile name

Storage pool name

5. Vous pouvez ajouter des périodes différentes ou créer des copies supplémentaires à différents emplacements :

- Sélectionnez l'icône plus pour créer des copies supplémentaires à un autre emplacement pendant la même période.
- Sélectionnez **Ajouter** pour ajouter une période différente aux instructions de placement.



Les objets sont automatiquement supprimés à la fin de la période finale, sauf si la période finale se termine par **Forever**.

6. Pour stocker des objets dans un pool de stockage cloud :

- Dans la liste déroulante **Type**, sélectionnez **Replicated**.
- Dans le champ **emplacement**, sélectionnez **Ajouter un pool**. Ensuite, sélectionnez un pool de stockage cloud.

From day 365 store forever Add Remove

Type replicated Location Example Cloud Storage Pool Add Pool Copies 1 + x

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.

Type replicated Location testpool2 testpool3 Add Pool Copies 1

If you want to use a Cloud Storage Pool, you must remove any other storage pools or Cloud Storage Pools from this placement instruction.

- 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.

Type replicated Location testpool Add Pool Copies 2

The number of copies cannot be more than one when a Cloud Storage Pool is selected.

- 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.

Placements [?](#) Sort by start day

From day store for days [Add](#) [Remove](#)

Type Location [Add Pool](#) Copies + x

Type Location [Add Pool](#) Copies + x

A rule cannot store more than one object copy in any Cloud Storage Pool at the same time. You must remove one of the Cloud Storage Pools (csp1, csp2) or use multiple placement instructions with dates that do not overlap. **Overlapping days:** 0-10.

To see the overlapping days on the Retention Diagram, click Refresh.

Retention Diagram [?](#) [Refresh](#)

- Vous pouvez stocker un objet dans un pool de stockage cloud simultanément dans lequel celui-ci est stocké sous forme de copies répliquées ou avec code d'effacement dans StorageGRID. Toutefois, comme le montre cet exemple, vous devez inclure plusieurs lignes dans l'instruction de placement pour la période de temps, de sorte que vous puissiez spécifier le nombre et les types de copies pour chaque emplacement.

Placements [?](#)

From day store for days

Type Location [Add Pool](#) Copies

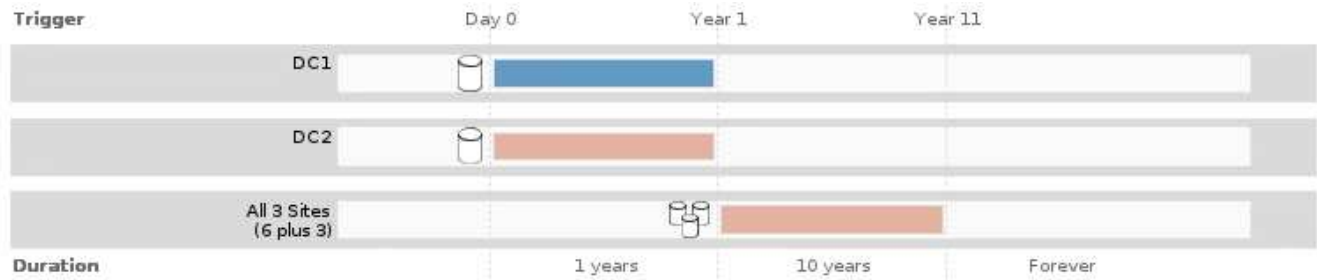
Type Location [Add Pool](#) Copies

- Sélectionnez **Actualiser** pour mettre à jour le diagramme de conservation et confirmer vos instructions de placement.

Chaque ligne du diagramme indique où et quand les copies d'objet seront placées. Le type de copie est représenté par l'une des icônes suivantes :

	La copie répliquée
	Copie avec code d'effacement
	Copie du pool de stockage cloud

Dans cet exemple, deux copies répliquées seront enregistrées sur deux pools de stockage (DC1 et DC2) pendant un an. Ensuite, une copie avec code d'effacement sera économisée pendant 10 ans supplémentaires et sera recourir à un schéma de code d'effacement 6+3 sur trois sites. Au bout de 11 ans, les objets seront supprimés de StorageGRID.



8. Sélectionnez **Suivant**.

L'étape 3 (définir le comportement d'ingestion) s'affiche.

Informations associées

- [Définition d'une règle ILM](#)
- [Gestion des objets avec le verrouillage d'objets S3](#)
- [Étape 3 sur 3 : définir le comportement d'entrée](#)

Utiliser l'heure du dernier accès dans les règles ILM

Vous pouvez utiliser l'heure du dernier accès comme heure de référence dans une règle ILM. Il peut par exemple être nécessaire de conserver les objets qui ont été affichés au cours des trois derniers mois sur les nœuds de stockage locaux tout en déplaçant des objets qui n'ont pas été considérés comme récemment vers un emplacement hors site. Vous pouvez également utiliser l'heure du dernier accès comme filtre avancé si vous souhaitez qu'une règle ILM s'applique uniquement aux objets qui ont été consultés pour la dernière fois à une date donnée.

Description de la tâche

Avant d'utiliser l'heure du dernier accès dans une règle ILM, prenez en compte les éléments suivants :

- 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 d'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 ce temps de latence en compte lors de la création de règles ILM basées sur le temps 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 dernières mises à jour des temps d'accès pour les compartiments S3. Vous pouvez utiliser le Gestionnaire de locataires ou l'API de gestion des locataires.



Les mises à jour du dernier accès sont toujours activées pour les conteneurs Swift, mais désactivées par défaut pour les compartiments S3.



Notez qu'en activant les mises à jour du dernier accès, vous pouvez réduire les performances, en particulier dans les systèmes dotés d'objets de petite taille. L'impact sur les performances a lieu, car StorageGRID doit mettre à jour les objets avec un nouvel horodatage chaque fois que les objets sont récupérés.

Le tableau suivant indique si l'heure du dernier accès est mise à jour pour tous les objets du compartiment pour différents types de requêtes.

Type de demande	Si l'heure du dernier accès est mise à jour lorsque les dernières mises à jour des temps d'accès sont désactivées	Si l'heure du dernier accès est mise à jour lorsque les dernières mises à jour des temps d'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

Informations associées

- [Utilisation de S3](#)
- [Utilisez un compte de locataire](#)

Étape 3 sur 3 : définir le comportement d'entrée

L'étape 3 (définir le comportement d'entrée) de l'assistant de création de règles ILM permet de choisir le mode de protection des objets filtrés par cette règle 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.

Create ILM Rule Step 3 of 3: Define ingest behavior

Select the data protection option to use when objects are ingested:

- ☐ Strict
Always uses this rule's placements on ingest. Ingest fails when this rule's placements are not possible.
- ☒ **Balanced**
Optimum ILM efficiency. Attempts this rule's placements on ingest. Creates interim copies when that is not possible.
- ☐ Dual commit
Creates interim copies on ingest and applies this rule's placements later.

Cancel Back Save

Étapes

1. Sélectionnez l'option de protection des données à utiliser lors de l'ingestion des objets :

Option	Description
Stricte	Utilise toujours les placements de cette règle lors de l'entrée. L'entrée échoue lorsque les placements de cette règle ne sont pas possibles.
Équilibré	Efficacité ILM optimale. Tente les placements de cette règle lors de l'entrée. Crée des copies intermédiaires lorsqu'elles ne sont pas possibles.
Double allocation	Crée des copies intermédiaires lors de l'entrée et applique ultérieurement les placements de cette règle.

Balance offre une combinaison de sécurité et d'efficacité des données adaptée dans la plupart des cas. En règle générale, une double validation est utilisée pour répondre à des exigences spécifiques.

Voir [Options de protection des données pour l'ingestion](#) et [Avantages, inconvénients et limites des options de protection des données](#) pour en savoir plus.



Un message d'erreur s'affiche si vous sélectionnez l'option stricte ou équilibrée et que la règle utilise l'un de ces placements :

- Un pool de stockage cloud dès le premier jour
- Un nœud d'archivage au jour 0
- Un pool de stockage dans le cloud ou un nœud d'archivage lorsque la règle utilise une heure de création définie par l'utilisateur comme heure de référence

2. Sélectionnez **Enregistrer**.

La règle ILM est enregistrée. La règle ne devient pas active tant qu'elle n'est pas ajoutée à une politique ILM et que cette règle est activée.

Informations associées

- [Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict](#)
- [Création d'une règle ILM](#)

Créez une règle ILM par défaut

Avant de créer une règle ILM, vous devez créer une règle par défaut afin de placer tous les objets qui ne correspondent pas à une autre règle de la politique. La règle par défaut ne peut pas utiliser de filtres. Elle doit s'appliquer à tous les locataires, à tous les compartiments et à toutes les versions d'objet.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

La règle par défaut est la dernière règle à évaluer dans une stratégie ILM. Elle ne peut donc pas utiliser de filtres ou l'heure de référence non actuelle. Les instructions de positionnement de la règle par défaut sont

appliquées à tous les objets qui ne sont pas mis en correspondance par une autre règle de la stratégie.

Dans cet exemple de politique, la première règle s'applique uniquement aux objets appartenant au locataire A. La règle par défaut, qui est la dernière, s'applique aux objets appartenant à tous les autres comptes de tenant.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Example ILM policy

Reason for change

Example policy

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

Default	Rule Name	Tenant Account	Actions
	EC for Tenant A	Tenant A (91643888913299990564)	✕
✓	2 copies 2 sites	—	✕

Cancel

Save

Lorsque vous créez la règle par défaut, gardez ces exigences à l'esprit :

- La règle par défaut est automatiquement placée en tant que dernière règle de la stratégie.
- La règle par défaut ne peut pas utiliser de filtres de base ou avancés.
- La règle par défaut doit s'appliquer à toutes les versions d'objet, de sorte qu'elle ne peut pas utiliser l'heure de référence non courante.
- 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 pour une règle. Les règles de code d'effacement doivent utiliser un filtre avancé pour empêcher le codage d'effacement des objets de petite taille.

- En général, la règle par défaut doit conserver les objets à tout jamais.
- Si vous utilisez (ou si vous prévoyez d'activer) le paramètre de verrouillage d'objet S3 global, la règle par défaut de la stratégie active ou proposée doit être conforme.

Étapes

1. Sélectionnez **ILM règles**.

La page règles ILM s'affiche.

2. Sélectionnez **Créer**.

L'étape 1 (définir les bases) de l'assistant Créer une règle ILM s'affiche.

3. Entrez un nom unique pour la règle dans le champ **Nom**.
4. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.
5. Laissez le champ **comptes locataire** vide.

La règle par défaut doit s'appliquer à tous les comptes de tenant.

6. Laissez le champ **Nom du compartiment** vide.

La règle par défaut doit s'appliquer à tous les compartiments S3 et les conteneurs Swift.

7. Ne sélectionnez pas **filtrage avancé**

La règle par défaut ne peut pas spécifier de filtres.

8. Sélectionnez **Suivant**.

L'étape 2 (définir les Placements) s'affiche.

9. Pour l'heure de référence, sélectionnez n'importe quelle option, à l'exception de **heure non actuelle**.

La règle par défaut doit appliquer toutes les versions d'objet.

10. 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 pour une règle. Les règles de codage d'effacement doivent inclure le filtre avancé **Object Size (MB) supérieur à 0.2** pour empêcher le codage d'effacement des objets plus petits.

- Si vous utilisez (ou si vous avez l'intention d'activer) le paramètre global de verrouillage d'objet S3, la règle par défaut doit être conforme :
 - Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
 - Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
 - Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
 - Les copies d'objet ne peuvent pas être enregistrées sur les nœuds d'archivage.
 - Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant l'heure d'ingestion comme heure de référence.
 - Au moins une ligne des instructions de placement doit être ""permanente".

11. Sélectionnez **Actualiser** pour mettre à jour le diagramme de conservation et confirmer vos instructions de placement.

12. Sélectionnez **Suivant**.

L'étape 3 (définir le comportement d'ingestion) s'affiche.

13. Sélectionnez l'option de protection des données à utiliser lors de l'ingestion d'objets et sélectionnez **Enregistrer**.

Création de la règle ILM

Création de la règle ILM : présentation

Lorsque vous créez une règle ILM, vous commencez par sélectionner et organiser les règles ILM. Ensuite, vous vérifiez le comportement de votre stratégie proposée en la simulant contre des objets précédemment ingérés. Lorsque vous êtes satisfait du fait que la stratégie proposée fonctionne comme prévu, vous pouvez l'activer pour créer la stratégie active.



Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Facteurs à prendre en compte lors de la création d'une règle ILM

- Vous pouvez utiliser la règle intégrée du système, la règle de base 2 copies, dans les systèmes de test uniquement. La règle de création de 2 copies 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.
- 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, cette règle ne sera pas évaluée par une autre règle.
- La dernière règle de chaque politique ILM est la règle ILM par défaut, qui ne peut utiliser aucun filtre. Si un objet n'a pas été mis en correspondance par une autre règle, la règle par défaut contrôle l'emplacement de cet objet et la durée de conservation.
- Avant d'activer une nouvelle stratégie, vérifiez les modifications apportées par la stratégie au placement des objets existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Création d'une règle ILM proposée

Vous pouvez créer de zéro une politique ILM proposée ou cloner la règle active actuelle si vous souhaitez commencer avec le même ensemble de règles.



Si le paramètre de verrouillage d'objet S3 global a été activé, utilisez plutôt cette procédure : [Créez une règle ILM après l'activation du verrouillage d'objet S3](#).

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez créé les règles ILM à ajouter à la règle proposée. Si nécessaire, vous pouvez enregistrer une stratégie proposée, créer des règles supplémentaires, puis modifier la stratégie proposée pour ajouter les nouvelles règles.
- Vous avez [Une règle ILM par défaut a été créée](#) pour la stratégie qui ne contient aucun filtre.
- Vous pouvez également regarder la vidéo : "[Vidéo : règles ILM de StorageGRID](#)"



Description de la tâche

Les raisons principales de la création d'une politique ILM sont les suivantes :

- Vous avez ajouté un site et devez utiliser de nouvelles règles ILM pour placer les objets sur ce site.
- Vous désaffectez un site et vous devez supprimer toutes les règles qui font référence au site.
- Vous avez ajouté un nouveau locataire qui présente des exigences spéciales de protection des données.
- Vous avez commencé à utiliser un pool de stockage cloud.



Vous pouvez utiliser la règle intégrée du système, la règle de base 2 copies, dans les systèmes de test uniquement. La règle de création de 2 copies de cette règle utilise le pool de stockage tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.

Étapes

1. Sélectionnez **ILM Policies**.

La page ILM Policies s'affiche. À partir de cette page, vous pouvez consulter la liste des stratégies proposées, actives et historiques ; créer, modifier, vous pouvez aussi supprimer une règle proposée, cloner la politique active ou afficher les détails d'une règle.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy
Clone
Edit
Remove

Policy Name	Policy State	Start Date	End Date
Baseline 2 Copies Policy	Active	2017-07-17 12:00:45 MDT	

Viewing Active Policy - Baseline 2 Copies Policy

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Make 2 Copies	✓	Ignore

Simulate
Activate

2. Déterminez le mode de création de la règle ILM proposée.

Option	Étapes
Créer une nouvelle règle proposée sans règles déjà sélectionnées	a. Si une stratégie ILM proposée existe actuellement, sélectionnez cette stratégie et sélectionnez Supprimer. Vous ne pouvez pas créer une nouvelle stratégie proposée si une stratégie proposée existe déjà. b. Sélectionnez Créer une stratégie proposée.
Création d'une règle proposée basée sur la règle active	a. Si une stratégie ILM proposée existe actuellement, sélectionnez cette stratégie et sélectionnez Supprimer. Vous ne pouvez pas cloner la règle active si une règle proposée existe déjà. b. Sélectionnez la stratégie active dans le tableau. c. Sélectionnez Clone.
Modifier la règle proposée existante	a. Sélectionnez la stratégie proposée dans le tableau. b. Sélectionnez Modifier.

La boîte de dialogue configurer la règle ILM s'affiche.

Si vous créez une nouvelle stratégie proposée, tous les champs sont vides et aucune règle n'est sélectionnée.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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

Default	Rule Name	Tenant Account	Actions

No rules selected.

Cancel

Save

Si vous clonez la politique active, le champ **Nom** affiche le nom de la règle active, ajouté par un numéro de version (« v2 » dans l'exemple). Les règles utilisées dans la stratégie active sont sélectionnées et affichées dans leur ordre actuel.

Name

Baseline 2 Copies Policy (v2)

Reason for change

3. Entrez un nom unique pour la stratégie proposée dans le champ **Nom**.

Vous devez entrer au moins 1 caractère et pas plus de 64 caractères. Si vous clonez la règle active, vous pouvez utiliser le nom actuel avec le numéro de version ajouté ou entrer un nouveau nom.

4. Entrez la raison pour laquelle vous créez une nouvelle stratégie proposée dans le champ **motif de changement**.

Vous devez entrer au moins 1 caractère et pas plus de 128 caractères.

5. Pour ajouter des règles à la stratégie, sélectionnez **Sélectionner les règles**.

La boîte de dialogue Sélectionner les règles pour la stratégie s'affiche, avec toutes les règles définies répertoriées. 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 utilisait un filtre ou l'heure de référence non actuelle, vous êtes invité à sélectionner une nouvelle règle par défaut.
- Si la règle par défaut n'était pas la dernière règle, un bouton vous permet de déplacer la règle vers la fin de la nouvelle stratégie.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

	Rule Name
☒	2 copies 2 sites
☐	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, advanced filter, or the noncurrent reference time).

	Rule Name	Tenant Account
☐	EC for Tenant A	Tenant A (91643888913299990564)
☐	2 copies 2 sites noncurrent time	—

Cancel

Apply

6. Sélectionnez un nom de règle ou l'icône plus de détails pour afficher les paramètres de cette règle.

Cet exemple présente le détail d'une règle ILM qui effectue deux copies répliquées sur deux sites.

Two-Site Replication for Other Tenants

Description:

Two-Site Replication for Other Tenants

Ingest Behavior:

Balanced

Reference Time:

Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:

Trigger

Day 0

DC1

DC2

Duration

Forever

Close

7. Dans la section **Sélectionner la règle par défaut**, sélectionnez une règle par défaut pour la stratégie proposée.

La règle par défaut s'applique à tous les 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.



Si aucune règle n'est répertoriée dans la section Sélectionner la règle par défaut, vous devez quitter la page de stratégie ILM et [Créer une règle ILM par défaut](#).



N'utilisez pas la règle de stock Make 2 copies comme règle par défaut pour une police. 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.

8. Dans la section **Sélectionner autres règles**, sélectionnez les autres règles que vous souhaitez inclure dans la stratégie.

Les autres règles sont évaluées avant la règle par défaut et doivent utiliser au moins un filtre (compte du locataire, nom du compartiment, filtre avancé ou heure de référence non actuelle).

9. Lorsque vous avez terminé de sélectionner des règles, sélectionnez **appliquer**.

Les règles que vous avez sélectionnées sont répertoriées. La règle par défaut est à la fin, avec les autres règles au-dessus.

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

	Default	Rule Name	Tenant Account	Actions
⬆⬇⬆	☐	3-site EC	Ignore	✕
⬆⬇⬆	☐	1-site EC	Ignore	✕
	☒	2 copies at 2 data centers	Ignore	✕

Cancel
Save

Un avertissement s'affiche si la règle par défaut ne conserve pas les objets pour toujours. Lorsque vous activez cette règle, vous devez confirmer que vous souhaitez que StorageGRID supprime des objets lorsque les instructions de placement de la règle par défaut s'écoulent (à moins qu'un cycle de vie du compartiment ne conserve les objets plus longtemps).



Default	Rule Name	Tenant Account	Actions
⬆⬇⬆	3-site EC	Ignore	✕
⬆⬇⬆	1-site EC	Ignore	✕
☒	2 copies at 2 data centers for 2 years	Ignore	✕

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 720 days.

10. Faites glisser et déposez les lignes des règles autres que celles par défaut pour déterminer l'ordre dans lequel ces règles seront évaluées.

Vous ne pouvez pas déplacer la règle par défaut.



Vous devez confirmer que les règles ILM sont dans l'ordre correct. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut.

11. Si nécessaire, sélectionnez l'icône de suppression ✖ Pour supprimer toutes les règles que vous ne souhaitez pas inclure dans la stratégie, ou sélectionnez **Sélectionner les règles** pour ajouter d'autres règles.
12. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

La page ILM de NetApp est mise à jour :

- La règle que vous avez enregistrée est affichée comme proposée. Les politiques proposées n'ont pas de dates de début et de fin.
- Les boutons **Simulate** et **Activate** sont activés.

13. Accédez à [Simulation d'une règle ILM](#).

Informations associées

- [Définition d'une règle ILM](#)
- [Gestion des objets avec le verrouillage d'objets S3](#)

Créez une règle ILM après l'activation du verrouillage d'objet S3

Si le paramètre global de verrouillage d'objet S3 est activé, les étapes de création d'une stratégie sont légèrement différentes. Vous devez vous assurer que la règle ILM est conforme aux exigences des compartiments dont l'option de verrouillage des objets S3 est activée.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Le paramètre global de verrouillage d'objet S3 est déjà activé pour le système StorageGRID.



Si le paramètre de verrouillage d'objet S3 global n'a pas été activé, suivez les instructions générales pour [Création d'une politique ILM proposée](#).

- Vous avez créé les règles ILM conformes et non conformes que vous souhaitez ajouter à la politique proposée. Si nécessaire, vous pouvez enregistrer une stratégie proposée, créer des règles supplémentaires, puis modifier la stratégie proposée pour ajouter les nouvelles règles. Voir [Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3](#).
- Vous avez [Une règle ILM par défaut a été créée](#) de la règle qui est conforme.
- Vous pouvez également regarder la vidéo : "[Vidéo : règles ILM de StorageGRID](#)"



Étapes

1. Sélectionnez **ILM Policies**.

La page ILM Policies s'affiche. Si le paramètre global S3 Object Lock est activé, la page ILM Policies indique quelles règles ILM sont conformes.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy
Clone
Edit
Remove

Policy Name	Policy State	Start Date	End Date
Baseline 2 Copies Policy	Active	2021-02-04 01:04:29 MST	

Viewing Active Policy - Baseline 2 Copies Policy

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Rules are evaluated in order, starting from the top. The policy's default rule must be compliant.

Rule Name	Default	Compliant	Tenant Account
Make 2 Copies	✓	✓	Ignore

Simulate
Activate

2. Entrez un nom unique pour la stratégie proposée dans le champ **Nom**.

Vous devez entrer au moins 1 caractère et pas plus de 64 caractères.

3. Entrez la raison pour laquelle vous créez une nouvelle stratégie proposée dans le champ **motif de changement**.

Vous devez entrer au moins 1 caractère et pas plus de 128 caractères.

4. Pour ajouter des règles à la stratégie, sélectionnez **Sélectionner les règles**.

La boîte de dialogue Sélectionner les règles pour la stratégie s'affiche, avec toutes les règles définies répertoriées.

- La section Sélectionner la règle par défaut répertorie les règles qui peuvent être par défaut pour une stratégie conforme. Il comprend des règles conformes qui n'utilisent pas de filtres ou l'heure de

référence non actuelle.

- La section Sélectionner autres règles répertorie les autres règles compatibles et non conformes qui peuvent être sélectionnées pour cette stratégie.

Select Rules for Policy

Select Default Rule

This list shows the rules that are compliant and do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last.

	Rule Name
☐	Default Compliant Rule: Two Copies Two Data Centers
☐	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, advanced filter, or the noncurrent reference time).

	Rule Name	Compliant	Uses Filter	Is Selectable
☐	Compliant Rule: EC for bank-records bucket - Bank of AB C	✓	✓	Yes
☐	Non-Compliant Rule: Use Cloud Storage Pool			Yes

CancelApply

5. Sélectionnez un nom de règle ou l'icône plus de détails pour afficher les paramètres de cette règle.
6. Dans la section **Sélectionner la règle par défaut**, sélectionnez une règle par défaut pour la stratégie proposée.

Le tableau de cette section répertorie uniquement les règles qui sont conformes et n'utilisent aucun filtre.



Si aucune règle n'est répertoriée dans la section Sélectionner la règle par défaut, vous devez quitter la page de stratégie ILM et [Créer une règle ILM par défaut](#) c'est-à-dire conforme.



N'utilisez pas la règle de stock Make 2 copies comme règle par défaut pour une police. 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.

7. Dans la section **Sélectionner autres règles**, sélectionnez les autres règles que vous souhaitez inclure dans la stratégie.
 - a. Si vous avez besoin d'une règle « par défaut » différente pour les objets dans des compartiments S3 non conformes, vous pouvez sélectionner une règle non conforme qui n'utilise pas de filtre.

Par exemple, vous pouvez utiliser un pool de stockage cloud ou un nœud d'archivage pour stocker des objets dans des compartiments où le verrouillage d'objet S3 n'est pas activé.



Vous ne pouvez sélectionner qu'une règle non conforme qui n'utilise pas de filtre. Dès que vous sélectionnez une règle, la colonne **est sélectionnable** affiche **non** pour toute autre règle non compatible sans filtre.

- a. Sélectionnez toutes les autres règles conformes ou non conformes que vous souhaitez utiliser dans la stratégie.

Les autres règles doivent utiliser au moins un filtre (compte du locataire, nom de compartiment ou filtre avancé, par exemple la taille de l'objet).

8. Lorsque vous avez terminé de sélectionner les règles, sélectionnez **appliquer**.

Les règles que vous avez sélectionnées sont répertoriées. La règle par défaut est à la fin, avec les autres règles au-dessus. Si vous avez également sélectionné une règle "par défaut" non conforme, cette règle est ajoutée comme règle de second à dernier dans la politique.

Dans cet exemple, la dernière règle, 2 copies 2 centres de données, est la règle par défaut : elle est conforme et ne comporte aucun filtre. La règle seconde à dernière, Cloud Storage Pool, n'a pas de filtres mais elle n'est pas conforme.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name Compliant ILM Policy for S3 Object Lock

Reason for change Example policy

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 (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules				
Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	Bank of ABC (90767802913525281639)	✕
	Non-Compliant Rule: Use Cloud Storage Pool		Ignore	✕
✓	Default Compliant Rule: Two Copies Two Data Centers	✓	Ignore	✕

Cancel

Save

9. Faites glisser et déposez les lignes des règles autres que celles par défaut pour déterminer l'ordre dans lequel ces règles seront évaluées.

Vous ne pouvez pas déplacer la règle par défaut ou la règle "par défaut" non conforme.



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.

10. Si nécessaire, sélectionnez l'icône de suppression ✕ Pour supprimer les règles que vous ne souhaitez pas inclure dans la stratégie ou **Sélectionner les règles** pour ajouter d'autres règles.

11. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

La page ILM de NetApp est mise à jour :

- La règle que vous avez enregistrée est affichée comme proposée. Les politiques proposées n'ont pas de dates de début et de fin.
- Les boutons **Simulate** et **Active** sont activés.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

[+ Create Proposed Policy](#) [Clone](#) [Edit](#) [Remove](#)

Policy Name	Policy State	Start Date	End Date
☒ Compliant ILM Policy for S3 Object Lock	Proposed		
☐ Compliant ILM Policy	Active	2021-02-05 16:22:53 MST	
☐ Non-Compliant ILM policy	Historical	2021-02-05 15:17:05 MST	2021-02-05 16:22:53 MST
☐ Baseline 2 Copies Policy	Historical	2021-02-04 21:35:52 MST	2021-02-05 15:17:05 MST

Viewing Proposed Policy - Compliant ILM Policy for S3 Object Lock

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change:

Rules are evaluated in order, starting from the top. The policy's default rule must be compliant.

Rule Name	Default	Compliant	Tenant Account
Compliant Rule: EC for bank-records bucket - Bank of ABC 🔗		✓	Bank of ABC (90767802913525281639)
Non-Compliant Rule: Use Cloud Storage Pool 🔗			Ignore
Default Compliant Rule: Two Copies Two Data Centers 🔗	✓	✓	Ignore

[Simulate](#) [Activate](#)

12. Accédez à [Simulation d'une règle ILM](#).

Simulation d'une règle ILM

Vous devez simuler une stratégie proposée sur les objets de test avant d'activer la stratégie et de l'appliquer à vos données de production. La fenêtre de simulation fournit un environnement autonome qui permet de tester les stratégies avant leur activation et leur application aux données de l'environnement de production.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Un compartiment S3, une clé d'objet ou le conteneur Swift, ou un nom d'objet pour chaque objet que vous souhaitez tester, vous avez déjà ingéré ces objets.

Description de la tâche

Vous devez sélectionner soigneusement les objets que vous souhaitez tester pour la stratégie proposée. Pour simuler une stratégie en profondeur, vous devez tester au moins un objet pour chaque filtre de chaque règle.

Par exemple, si une règle inclut une règle permettant de faire correspondre des objets dans le compartiment A et une autre règle pour faire correspondre des objets dans le compartiment B, vous devez sélectionner au moins un objet du compartiment A et un objet du compartiment B pour tester la règle en profondeur. Vous devez également sélectionner au moins un objet d'un autre compartiment pour tester la règle par défaut.

Lors de la simulation d'une règle, les considérations suivantes s'appliquent :

- Après avoir apporté des modifications à une police, enregistrez la stratégie proposée. Ensuite, simulez le comportement de la stratégie proposée enregistrée.
- Lorsque vous simulez une règle, les règles ILM de la règle filtrent les objets test. Vous pouvez ainsi voir la règle appliquée à chaque objet. Cependant, aucune copie d'objet n'est effectuée et aucun objet n'est placé. L'exécution d'une simulation ne modifie en aucune façon vos données, règles ou règles.
- La page Simulation conserve les objets que vous avez testés jusqu'à ce que vous ferquiez, ne vous éloignez pas de la page règles ILM ou que vous la réactualisez.
- Simulation renvoie le nom de la règle lettrée. Pour déterminer quel pool de stockage ou profil de code d'effacement est en vigueur, vous pouvez afficher le diagramme de rétention en sélectionnant le nom de la règle ou l'icône plus de détails .
- Si le contrôle de version S3 est activé, la règle est uniquement simulée par rapport à la version actuelle de l'objet.

Étapes

1. Sélectionnez et organisez les règles, puis enregistrez la stratégie proposée.

La politique dans cet exemple comporte trois règles :

Nom de la règle	Filtre	Type de copies	La conservation
X-hommes	• Locataire A • Métadonnées utilisateur (série=x-men)	2 copies dans deux data centers	2 ans
PNG	Touche se termine par .png	2 copies dans deux data centers	5 ans
Deux copies pour les data centers	Aucun	2 copies dans deux data centers	Toujours

Viewing Proposed Policy - Example ILM policy

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
X-men 		Tenant A (94793396288150002349)
PNGs 		Ignore
Two Copies at Two Data Centers 	✓	Ignore

Simulate

Activate

2. Utilisation d'un client S3, Swift ou [Console S3 expérimentale](#), Disponible dans le Gestionnaire de locataires pour chaque locataire, ingèrent les objets requis pour tester chaque règle.

3. Sélectionnez **simuler**.

La boîte de dialogue règle ILM de simulation s'affiche.

4. Dans le champ **objet**, saisissez la clé de rubrique/objet S3 ou le nom-objet/conteneur Swift pour un objet test, puis sélectionnez **Simulate**.

Un message apparaît si vous spécifiez un objet qui n'a pas été ingéré.



Object

photos/test

Simulate

Object 'photos/test' not found.

5. Sous **Résultats de simulation**, confirmez que chaque objet a été mis en correspondance par la règle correcte.

Dans l'exemple, le `Havok.png` et `Warpath.jpg` Les objets ont été correctement mis en correspondance par la règle X-Men. Le `Fullsteam.png` objet, qui n'inclut pas `series=x-men` Les métadonnées utilisateur n'ont pas été mises en correspondance par la règle X-Men, mais elles ont été correctement mises en correspondance par la règle PNG. La règle par défaut n'a pas été utilisée car les trois objets étaient tous comparés par d'autres règles.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men 		✘
photos/Warpath.jpg	X-men 		✘
photos/Fullsteam.png	PNGs 		✘

Exemple 1 : vérifiez les règles lors de la simulation d'une règle ILM proposée

Cet exemple montre comment vérifier des règles lors de la simulation d'une règle proposée.

Dans cet exemple, la **exemple de règle ILM** est simulée contre les objets ingérés dans deux compartiments. La politique comprend trois règles, comme suit :

- La première règle, **deux copies, deux ans pour le compartiment a**, ne s'applique qu'aux objets du compartiment a.
- La seconde 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.

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See the [instructions for managing objects with ILM](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. Using EC is best suited for objects greater than 1 MB. See the [instructions for managing objects with ILM](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change:

Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Two copies, two years for bucket-a 		—
EC objects > 1 MB 		—
Two copies, two data centers 	✓	—

Simulate

Activate

Étapes

1. Après avoir ajouté les règles et enregistré la stratégie, sélectionnez **Simulate**.

La boîte de dialogue Simulate ILM Policy s'affiche.

2. Dans le champ **objet**, saisissez la clé de rubrique/objet S3 ou le nom-objet/conteneur Swift pour un objet test, puis sélectionnez **Simulate**.

Les résultats de la simulation s'affichent, indiquant quelle règle dans la stratégie correspond à chaque objet testé.

Simulate ILM Policy - Example ILM policy

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

[Simulate](#)

Simulation Results

Object	Rule Matched	Previous Match	
bucket-a/bucket-a object.pdf	Two copies, two years for bucket-a 		✗
bucket-b/test object greater than 1 MB.pdf	EC objects > 1 MB 		✗
bucket-b/test object less than 1 MB.pdf	Two copies, two data centers 		✗

[Finish](#)

3. Confirmez que chaque objet a été mis en correspondance par la règle correcte.

Dans cet exemple :

- bucket-a/bucket-a object.pdf correspondance correcte de la première règle, qui filtre les objets dans bucket-a.
- bucket-b/test object greater than 1 MB.pdf est dans bucket-b, il ne correspond donc pas à la première règle. Au lieu de cela, il a été correctement mis en correspondance par la deuxième règle, qui filtre les objets de plus de 1 Mo.
- bucket-b/test object less than 1 MB.pdf ne correspond pas aux filtres des deux premières règles. il sera donc placé par la règle par défaut, qui ne comprend aucun filtre.

Exemple 2 : règles de réorganisation lors de la simulation d'une règle ILM proposée

Cet exemple montre comment vous pouvez réorganiser les règles pour modifier les résultats lors de la simulation d'une règle.

Dans cet exemple, la politique **Demo** est en cours de simulation. Cette règle, qui vise à trouver des objets qui ont des métadonnées utilisateur série=x-men, comprend trois règles, comme suit :

- La première règle, **PNG**, filtre les noms de clé qui se terminent dans .png.
- La deuxième règle, **X-men**, ne s'applique qu'aux objets pour le locataire A et les filtres pour `series=x-men` métadonnées d'utilisateur.
- La dernière règle, **deux copies deux centres de données**, est la règle par défaut, qui correspond à tous les objets qui ne correspondent pas aux deux premières règles.

Viewing Proposed Policy - Demo

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: new policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
PNGs 		Ignore
X-men 		Tenant A (24365814597594524591)
Two copies two data centers 	✓	Ignore

SimulateActivate

Étapes

1. Après avoir ajouté les règles et enregistré la stratégie, sélectionnez **Simulate**.
2. Dans le champ **objet**, saisissez la clé de rubrique/objet S3 ou le nom-objet/conteneur Swift pour un objet test, puis sélectionnez **Simulate**.

Les résultats de la simulation s'affichent, indiquant que `Havok.png` L'objet a été associé à la règle **PNG**.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object Simulate

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	PNGs 		✗

Finish

Toutefois, la règle que le `Havok.png` L'objet était destiné à tester était la règle **X-Men**.

3. Pour résoudre le problème, réorganisez les règles.
 - a. Sélectionnez **Finish** pour fermer la page simuler la politique ILM.
 - b. Sélectionnez **Modifier** pour modifier la stratégie.
 - c. Faites glisser la règle **X-men** en haut de la liste.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name Demo

Reason for change Reordering rules when simulating a proposed ILM policy

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

	Default	Rule Name	Tenant Account	Actions
+		X-men	Tenant A (48713995194927812566)	✕
+		PNGs	—	✕
	✓	Two copies, two data centers	—	✕

Cancel

Save

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 règle mise en correspondance indique que `Havok.png` L'objet correspond désormais à la règle des métadonnées X-men, comme prévu. La colonne comparaison précédente indique que la règle des CNG correspond à l'objet dans la simulation précédente.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object my-bucket/my-object-name or my-container/my-object-name

Simulate

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men	PNGs	✕

Finish



Si vous restez sur la page configurer les stratégies, vous pouvez simuler une stratégie après avoir effectué des modifications sans avoir à saisir à nouveau les noms des objets de test.

Exemple 3 : corriger une règle lors de la simulation d'une politique ILM proposée

Cet exemple montre comment simuler une stratégie, corriger une règle dans la règle et poursuivre la simulation.

Dans cet exemple, la politique **Demo** est en cours de simulation. Cette politique a pour but de trouver des

objets qui ont `series=x-men` métadonnées d'utilisateur. Toutefois, des résultats inattendus se sont produits lors de la simulation de cette politique contre le `Beast.jpg` objet. Au lieu de faire correspondre la règle de métadonnées X-Men, l'objet correspond à la règle par défaut, deux copies de deux centres de données.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

my-bucket/my-object-name or my-container/my-object-name

Simulate

Simulation Results ?

Object	Rule Matched	Previous Match	
photos/Beast.jpg	Two copies two data centers		✖

Finish

Lorsqu'un objet test n'est pas associé à la règle attendue de la stratégie, vous devez examiner chaque règle de la stratégie et corriger les erreurs éventuelles.

Étapes

- 1. Pour chaque règle de la stratégie, affichez les paramètres de la règle en sélectionnant le nom de la règle ou l'icône plus de détails dans n'importe quelle boîte de dialogue où la règle est affichée.
- 2. Vérifiez le compte de locataire de la règle, l'heure de référence et les critères de filtrage.

Dans cet exemple, les métadonnées de la règle X-men comportent une erreur. La valeur des métadonnées a été saisie comme « x-men1 » au lieu de « x-men ».

X-men

Ingest Behavior:Balanced

Tenant Account:06846027571548027538

Reference Time:Ingest Time

Filtering Criteria:

Matches all of the following metadata:

User Metadata

series

equals

x-men1

Retention Diagram:

Trigger

Day 0

All Storage Nodes

Duration

Forever

Close

425

3. Pour résoudre l'erreur, corrigez la règle comme suit :

- Si la règle fait partie de la stratégie proposée, vous pouvez soit cloner la règle, soit supprimer la règle de la stratégie, puis la modifier.
- Si la règle fait partie de la stratégie active, vous devez cloner la règle. Vous ne pouvez pas modifier ou supprimer une règle de la stratégie active.

Option	Description
Clonez la règle	i. Sélectionnez ILM règles. ii. Sélectionnez la règle incorrecte et sélectionnez Clone. iii. Modifiez les informations incorrectes et sélectionnez Enregistrer. iv. Sélectionnez ILM Politiques. v. Sélectionnez la stratégie proposée et sélectionnez Modifier. vi. Sélectionnez Sélectionner règles. vii. Cochez la case de la nouvelle règle, décochez la case de la règle d'origine et sélectionnez appliquer. viii. Sélectionnez Enregistrer.
Modifiez la règle	i. Sélectionnez la stratégie proposée et sélectionnez Modifier. ii. Sélectionnez l'icône de suppression ✕ Pour supprimer la règle incorrecte et sélectionnez Enregistrer. iii. Sélectionnez ILM règles. iv. Sélectionnez la règle incorrecte et sélectionnez Modifier. v. Modifiez les informations incorrectes et sélectionnez Enregistrer. vi. Sélectionnez ILM Politiques. vii. Sélectionnez la stratégie proposée et sélectionnez Modifier. viii. Sélectionnez la règle corrigée, sélectionnez appliquer, puis Enregistrer.

4. Exécuter à nouveau la simulation.



Comme vous avez navigué loin de la page ILM Politiques pour modifier la règle, les objets que vous avez précédemment saisis pour la simulation ne sont plus affichés. Vous devez saisir à nouveau les noms des objets.

Dans cet exemple, la règle X-men corrigée correspond maintenant à l' `Beast.jpg` objet basé sur `series=x-men` les métadonnées d'utilisateur, comme prévu.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Beast.jpg	X-men 		

Activation de la règle ILM

Une fois que vous avez ajouté des règles ILM à une politique ILM proposée, que vous simulez la règle et que vous la confirmez, vous êtes prêt à activer la règle proposée.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez enregistré et simulé la règle ILM proposée.



Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets 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.

Description de la tâche

Lorsque vous activez une règle ILM, le système distribue la nouvelle règle à tous les nœuds. Cependant, la nouvelle règle active peut ne pas être appliquée tant que tous les nœuds du grid ne sont pas disponibles pour recevoir la nouvelle règle. Dans certains cas, le système attend d'implémenter une nouvelle stratégie active pour s'assurer que les objets de grille ne sont pas accidentellement supprimés.

- Si vous apportez des modifications de règles qui augmentent la redondance ou la durabilité des données, ces modifications sont immédiatement mises en œuvre. Par exemple, si vous activez une nouvelle règle incluant une règle à trois copies au lieu d'une règle à deux copies, cette règle sera immédiatement implémentée car elle accroît la redondance des données.
- Si vous apportez des modifications à des règles susceptibles de réduire la redondance ou la durabilité des données, ces modifications ne seront pas implémentées tant que tous les nœuds de la grille ne sont pas disponibles. Par exemple, si vous activez une nouvelle règle qui utilise une règle à deux copies au lieu d'une règle à trois copies, la nouvelle politique sera marquée comme « active », mais elle ne prendra effet qu'une fois que tous les nœuds seront en ligne et disponibles.

Étapes

1. Lorsque vous êtes prêt à activer une stratégie proposée, sélectionnez-la sur la page règles ILM et sélectionnez **Activer**.

Un message d'avertissement s'affiche, vous invitant à confirmer que vous souhaitez activer la stratégie proposée.

⚠ Warning

Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating. Are you sure you want to activate the proposed policy?

Cancel

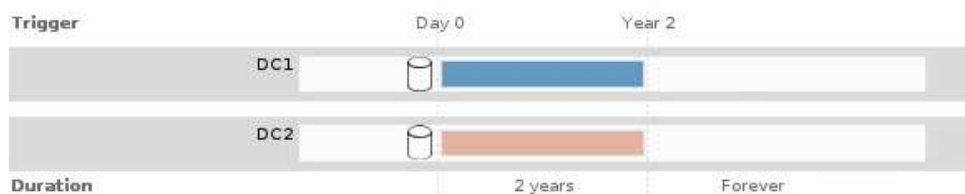
OK

Une invite apparaît dans le message d'avertissement si la règle par défaut de la stratégie ne conserve pas les objets indéfiniment. Dans cet exemple, le diagramme de conservation montre que la règle par défaut supprimera les objets après 2 ans. Vous devez taper **2** dans la zone de texte pour confirmer que tous les objets qui ne correspondent pas à une autre règle de la stratégie seront supprimés de StorageGRID après 2 ans.

⚠ Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating.

The default rule in this policy does not retain objects forever. Confirm this is the behavior you want by referring to the retention diagram for the default rule:



Now, complete the following prompt:

Any objects that are not matched by another rule in this policy will be deleted after years.

Are you sure you want to activate the proposed policy?

Cancel

OK

2. Sélectionnez **OK**.

Résultat

Lorsqu'une nouvelle règle ILM a été activée :

- La règle est affichée avec un état de règle actif dans le tableau de la page ILM Politiques. L'entrée Date de début indique la date et l'heure d'activation de la stratégie.

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy Clone Edit Remove			
Policy Name	Policy State	Start Date	End Date
☒ New Policy	Active	2017-07-20 18:49:53 MDT	
☐ Baseline 2 Copies Policy	Historical	2017-07-19 21:24:30 MDT	2017-07-20 18:49:53 MDT

- La stratégie précédemment active est affichée avec un état de police de l'historique. Les entrées Date de début et Date de fin indiquent quand la police est devenue active et quand elle n'était plus en vigueur.

Informations associées

Exemple 6 : modification d'une règle ILM

Vérification d'une règle ILM avec la recherche de métadonnées d'objet

Une fois la règle ILM activée, vous devez ingérer des objets test représentatifs dans le système StorageGRID. Vous devez ensuite effectuer une recherche de métadonnées d'objet pour confirmer que les copies sont effectuées comme prévu et placées aux emplacements appropriés.

Ce dont vous avez besoin

- Vous disposez d'un identificateur d'objet, qui peut être l'un des suivants :
 - UUID** : identifiant unique universel de l'objet. Saisissez l'UUID en majuscules.
 - CBID** : identifiant unique de l'objet dans StorageGRID. Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.
 - Compartiment S3 et clé d'objet** : lors de l'ingestion d'un objet via l'interface S3, l'application client utilise une combinaison de compartiments et de clés d'objet pour stocker et identifier l'objet. Si le compartiment S3 est avec version et que vous souhaitez rechercher une version spécifique d'un objet S3 à l'aide du compartiment et de la clé d'objet, vous disposez de l'**ID version**.
 - Conteneur Swift et nom d'objet** : lorsqu'un objet est ingéré via l'interface Swift, l'application cliente utilise une combinaison de conteneur et de nom d'objet pour stocker et identifier l'objet.

Étapes

- Ingestion de l'objet.
- Sélectionnez **ILM recherche métadonnées objet**.
- Saisissez l'identifiant de l'objet dans le champ **Identificateur**. Vous pouvez entrer un UUID, un CBID, un compartiment S3/une clé-objet ou un nom-objet/conteneur Swift.
- Si vous le souhaitez, entrez un ID de version pour l'objet (S3 uniquement).

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Version ID
(optional)

Look Up

5. Sélectionnez **rechercher**.

Les résultats de la recherche de métadonnées d'objet s'affichent. Cette page répertorie les types d'informations suivants :

- Les métadonnées du système, y compris l'ID d'objet (UUID), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAHS": "2",

```

6. Vérifiez que l'objet est stocké à l'emplacement ou aux emplacements appropriés et qu'il s'agit du type de copie correct.



Si l'option Audit est activée, vous pouvez également surveiller le journal d'audit du message règles objet respectées ORLM. Le message d'audit ORLM peut vous fournir plus d'informations sur l'état du processus d'évaluation ILM, mais il ne peut pas vous fournir des informations sur l'exactitude du placement des données d'objet ou l'exhaustivité de la politique ILM. Vous devez évaluer cela vous-même. Pour plus de détails, voir [Examiner les journaux d'audit](#).

Informations associées

- [Utilisation de S3](#)
- [Utiliser Swift](#)

Utilisation des règles ILM et des règles ILM

Une fois que vous avez créé des règles ILM et une règle ILM, vous pouvez continuer à

travailler avec elles, en modifiant leur configuration au fur et à mesure de l'évolution de vos besoins en stockage.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Supprime une règle ILM

Pour que la liste des règles ILM actuelles puisse être gérée, supprimez les règles ILM que vous ne pensez pas utiliser.

Vous ne pouvez pas supprimer une règle ILM si elle est actuellement utilisée dans la politique active ou la politique proposée. Si vous avez besoin de supprimer une règle ILM utilisée, vous devez d'abord effectuer la procédure suivante :

1. Clonez la règle active ou modifiez la règle proposée.
2. Supprimez la règle ILM de la règle.
3. Enregistrez, simulez et activez la nouvelle stratégie pour vous assurer que les objets sont protégés comme prévu.

Étapes

1. Sélectionnez **ILM règles**.
2. Vérifiez l'entrée de la table pour la règle que vous souhaitez supprimer.

Vérifiez que la règle n'est pas utilisée dans la politique ILM active ou la politique ILM proposée.

3. Si la règle que vous souhaitez supprimer n'est pas utilisée, sélectionnez le bouton radio et sélectionnez **Supprimer**.
4. Sélectionnez **OK** pour confirmer que vous souhaitez supprimer la règle ILM.

La règle ILM est supprimée.

Si vous supprimez une règle utilisée dans une stratégie historique, un  cette icône apparaît pour la règle lorsque vous affichez la stratégie, ce qui indique que la règle est devenue une règle historique.

Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name

Erasure code larger objects

2 copies 2 sites  

This is a historical ILM rule.
Historical rules are rules that
were included a policy and then
edited or deleted after the policy
became historical.

Modifiez une règle ILM

Vous devrez peut-être modifier une règle ILM pour modifier une instruction de filtre ou de placement.

Une règle ne peut pas être modifiée s'il est utilisé dans la politique ILM proposée ou la politique ILM active. Vous pouvez plutôt cloner ces règles et apporter les modifications nécessaires à la copie clonée. Vous ne pouvez pas non plus modifier la règle ILM (réalisation de 2 copies) ou les règles ILM créées avant la version 10.3 d'StorageGRID.



Avant d'ajouter une règle modifiée à la règle ILM active, notez que toute modification des instructions de placement d'un objet peut entraîner une charge croissante sur le système.

Étapes

1. Sélectionnez ILM règles.

La page règles ILM s'affiche. Cette page affiche toutes les règles disponibles et indique les règles utilisées dans la stratégie active ou la règle proposée.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

 Create  Edit  Clone  Remove			
Name	Used In Active Policy	Used In Proposed Policy	
☐ Make 2 Copies	✓	✓	
☐ PNGs		✓	
☒ JPGs			
☐ X-men		✓	

2. Sélectionnez une règle qui n'est pas utilisée et sélectionnez **Modifier**.

L'assistant Modifier la règle ILM s'ouvre.

Edit ILM Rule Step 1 of 3: Define Basics

Name: JPGs

Description:

Tenant Accounts (optional): Tenant-01 (16229710975421005503) Tenant-04 (83132053388229808098)

Bucket Name: contains az-01

Advanced filtering... (0 defined)

Cancel Next

3. Complétez les pages de l'assistant Modifier la règle ILM, en suivant les étapes de [Création d'une règle ILM](#) et [utilisation de filtres avancés](#), selon les besoins.

Lors de la modification d'une règle ILM, vous ne pouvez pas modifier son nom.

4. Sélectionnez **Enregistrer**.

Si vous modifiez une règle utilisée dans une stratégie historique, un ⓘ cette icône apparaît pour la règle lorsque vous affichez la stratégie, ce qui indique que la règle est devenue une règle historique.



Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name
Erasure code larger objects
2 copies 2 sites ⓘ

This is a historical ILM rule. Historical rules are rules that were included a policy and then edited or deleted after the policy became historical.

Cloner une règle ILM

Une règle ne peut pas être modifiée s'il est utilisé dans la politique ILM proposée ou la politique ILM active. Vous pouvez plutôt cloner une règle et apporter les modifications nécessaires à la copie clonée. Ensuite, si nécessaire, vous pouvez supprimer la règle d'origine de la stratégie proposée et la remplacer par la version modifiée. Cette règle ne peut pas être clonées s'il a été créée à l'aide de la version 10.2 de StorageGRID ou antérieure.

Avant d'ajouter une règle clonée à la règle ILM active, veuillez noter que la modification des instructions de placement d'un objet peut augmenter la charge appliquée au système.

Étapes

1. Sélectionnez **ILM règles**.

La page règles ILM s'affiche.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

+ Create Edit Clone Remove			
Name		Used In Active Policy	Used In Proposed Policy
☐	Make 2 Copies	✓	✓
☐	PNGs		✓
☒	JPGs		
☐	X-men		✓

2. Sélectionnez la règle ILM à cloner et sélectionnez **Clone**.

L'assistant Créer une règle ILM s'ouvre.

3. Mettez à jour la règle clonée en suivant les étapes de modification d'une règle ILM et d'utilisation des filtres avancés.

Lors du clonage d'une règle ILM, vous devez entrer un nouveau nom.

4. Sélectionnez **Enregistrer**.

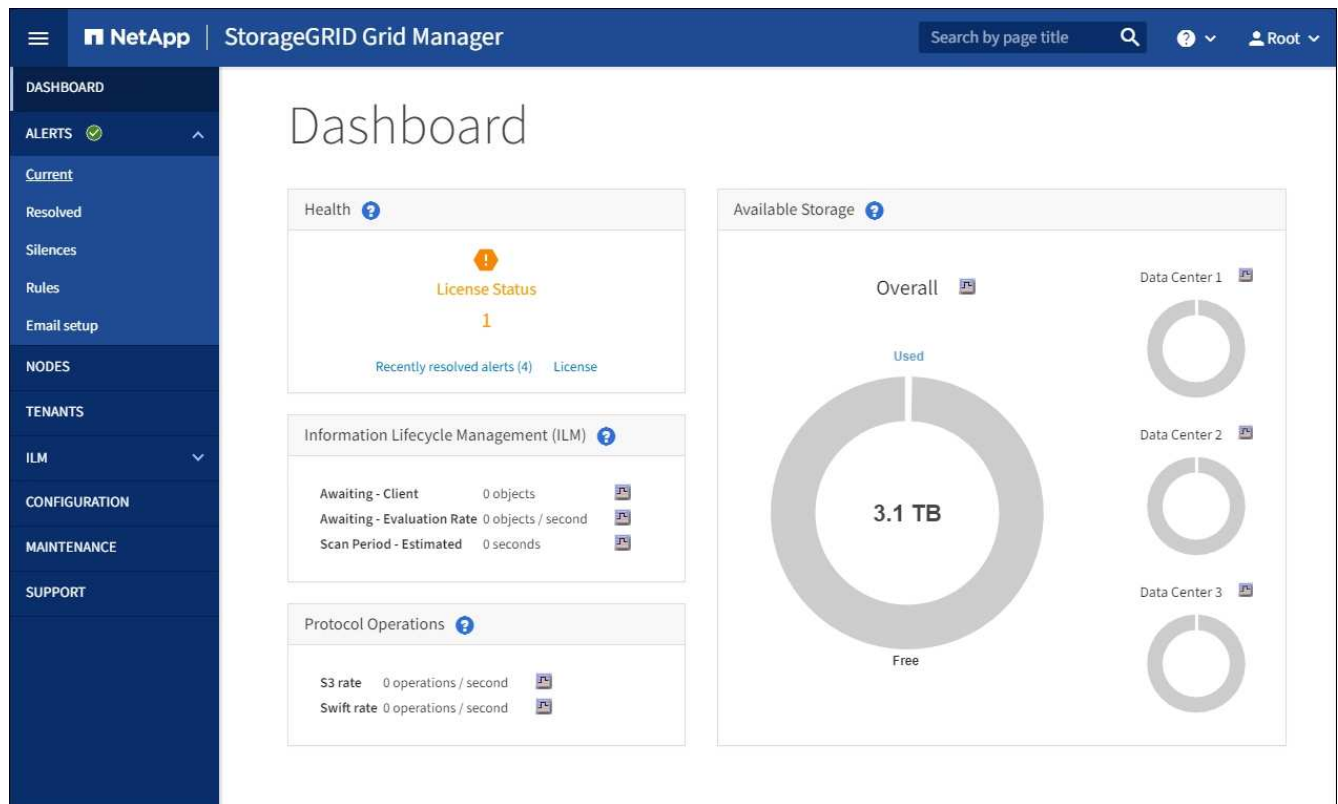
La nouvelle règle ILM est créée.

Affichez la file d'attente d'activité de la stratégie ILM

Vous pouvez à tout moment afficher le nombre d'objets de la file d'attente à évaluer par rapport à la règle ILM. Vous pouvez être susceptible de surveiller la file d'attente de traitement ILM pour déterminer les performances du système. Une grande file d'attente peut indiquer que le système n'est pas en mesure de suivre le taux d'entrée, que la charge des applications client est trop élevée ou qu'il existe un problème anormal.

Étapes

1. Sélectionnez **Tableau de bord**.



2. Surveillez la section gestion du cycle de vie de l'information (ILM).

Vous pouvez sélectionner le point d'interrogation ? pour voir une description des éléments de cette section.

Verrouillage des objets S3 avec ILM

Gestion des objets avec le verrouillage d'objets S3

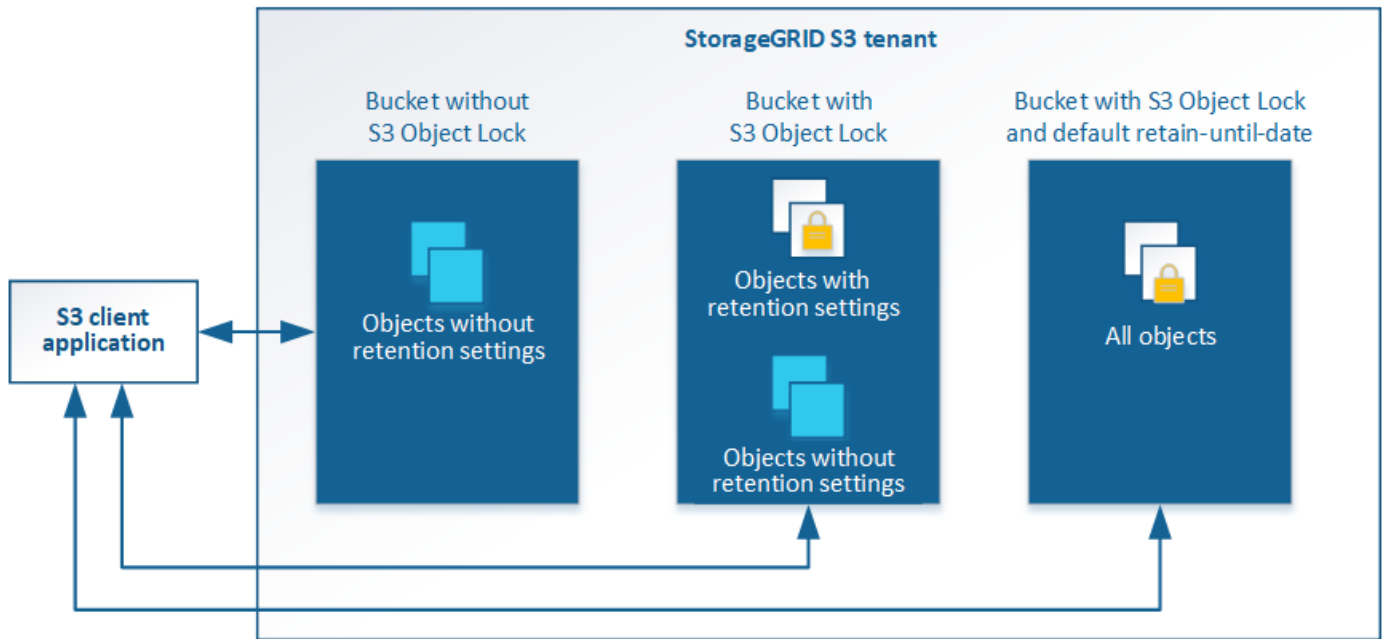
En tant qu'administrateur de la grille, vous pouvez activer la fonction de verrouillage des objets S3 pour votre système StorageGRID et mettre en œuvre une règle ILM conforme pour vous assurer que les objets des compartiments S3 spécifiques ne sont pas supprimés ou remplacés pour une durée spécifiée.

Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si un compartiment est doté du verrouillage objet S3 activé, les applications client S3 peuvent éventuellement spécifier des paramètres de conservation pour toute version d'objet dans ce compartiment. Des paramètres de conservation doivent être spécifiés pour être protégés par le verrouillage d'objet S3. En outre, chaque compartiment sur lequel le verrouillage d'objet S3 est activé peut avoir la possibilité de disposer d'un mode de conservation et d'une période de conservation par défaut, qui s'appliquent si des objets sont ajoutés au compartiment sans leurs propres paramètres de conservation.

StorageGRID with S3 Object Lock setting enabled



La fonctionnalité de verrouillage d'objet StorageGRID S3 fournit un mode de conservation unique équivalent au mode de conformité Amazon S3. Par défaut, une version d'objet protégé ne peut être écrasée ou supprimée par aucun utilisateur. La fonction de verrouillage d'objet StorageGRID S3 ne prend pas en charge un mode de gouvernance et n'autorise pas les utilisateurs disposant d'autorisations spéciales à contourner les paramètres de rétention ou à supprimer des objets protégés.

Si un compartiment est doté de l'option de verrouillage des objets S3, l'application client S3 peut spécifier la ou les deux paramètres de conservation de niveau objet suivants lors de la création ou de la mise à jour d'un objet :

- **Conserver-jusqu'à-date** : si la date-à-jour d'une version d'objet est à l'avenir, l'objet peut être récupéré, mais ne peut pas être modifié ou supprimé. Si nécessaire, la date de conservation d'un objet peut être augmentée, mais cette date ne peut pas être réduite.
- **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.

Pour plus d'informations sur les paramètres de conservation des objets, reportez-vous à la section [Utilisez le verrouillage d'objet S3](#).

Pour plus d'informations sur les paramètres de conservation des compartiments par défaut, accédez à [Utilisez la conservation de compartiment par défaut avec le verrouillage d'objet S3](#).

Comparaison du verrouillage d'objet S3 à la conformité existante

Le verrouillage d'objet S3 remplace la fonctionnalité de conformité disponible dans les versions précédentes de StorageGRID. La fonctionnalité de verrouillage d'objet S3 conforme aux exigences Amazon S3 représente la fonctionnalité propriétaire de conformité StorageGRID, appelée désormais « conformité héritée ».

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre global de verrouillage d'objet S3 a été activé automatiquement. Les locataires ne peuvent plus créer de compartiments avec la

conformité activée. Toutefois, si nécessaire, les locataires peuvent continuer à utiliser et à gérer n'importe quelle version existante de conformité, notamment effectuer les tâches suivantes :

- Ingestion de nouveaux objets dans un compartiment pour lequel la conformité d'ancienne génération est activée.
- Augmentation de la période de conservation d'un compartiment existant pour lequel la conformité des données héritées est activée.
- Modification du paramètre de suppression automatique pour un compartiment existant sur lequel la conformité héritée est activée.
- Placer la conservation légale sur un compartiment existant pour lequel la conformité héritée est activée.
- Levée d'une suspension légale.

Voir "[Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5](#)" pour obtenir des instructions.

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.

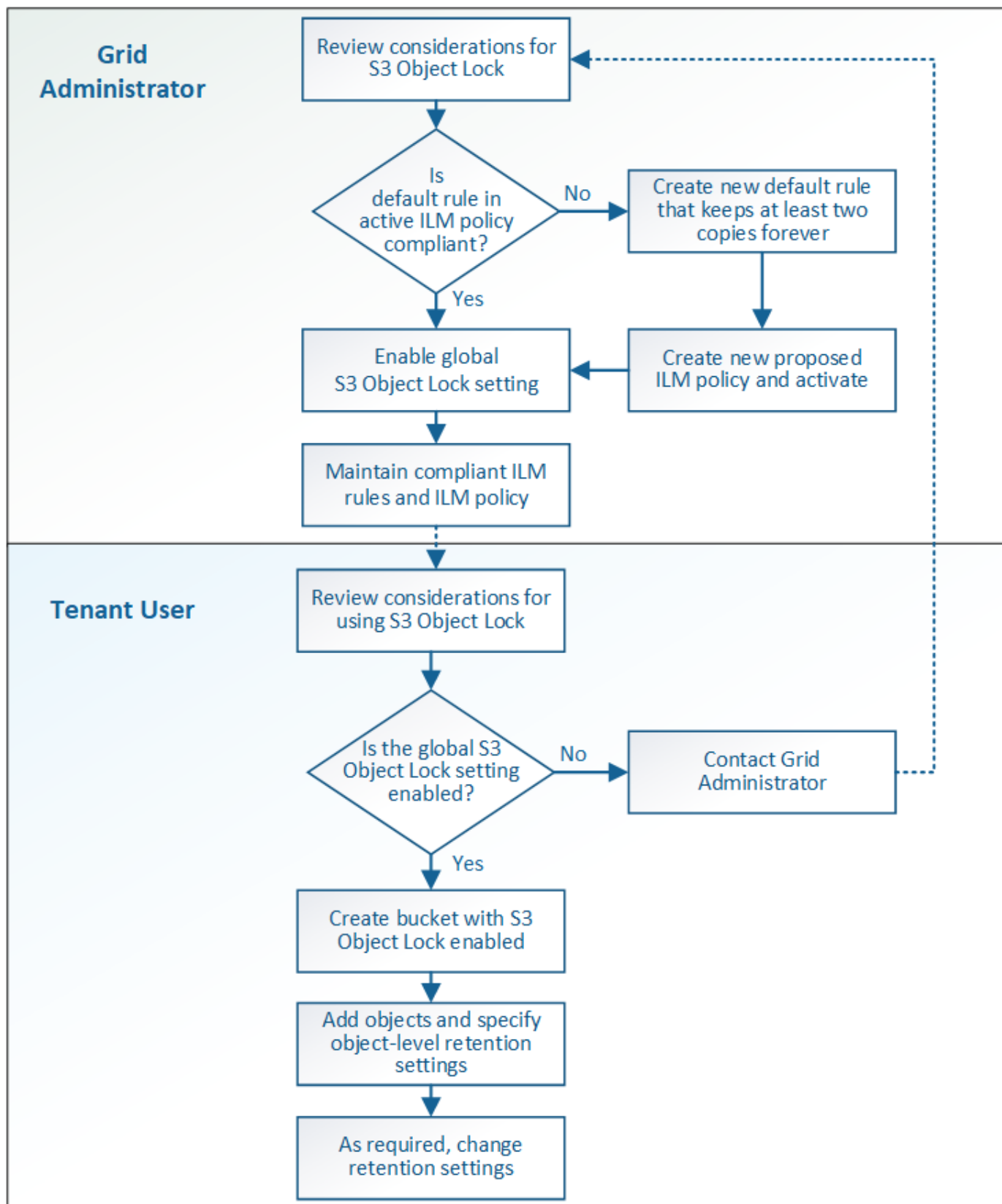
	Verrouillage objet S3 (nouveau)	Conformité (existant)
Comment cette fonctionnalité est-elle activée dans le monde entier ?	Dans Grid Manager, sélectionnez CONFIGURATION système verrouillage objet S3 .	N'est plus pris en charge. Remarque : si vous avez activé le paramètre de conformité globale à l'aide d'une version précédente de StorageGRID, le paramètre verrouillage d'objet S3 est activé dans StorageGRID 11.6. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants. Cependant, vous ne pouvez pas créer de compartiments conformes.
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.	Les utilisateurs ne peuvent plus créer de compartiments avec la conformité activée. Toutefois, ils peuvent continuer à ajouter de nouveaux objets aux compartiments conformes existants.
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 La fonction de conformité héritée n'autorise pas la gestion des versions de compartiment.

	Verrouillage objet S3 (nouveau)	Conformité (existant)
Comment la conservation d'objets est-elle définie ?	Les utilisateurs peuvent définir une date de conservation pour chaque version d'objet.	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.
Un compartiment peut-il disposer de paramètres par défaut pour la conservation des données et la conservation à des fins juridiques ?	Oui. Les compartiments StorageGRID sur lesquels le verrouillage d'objet S3 est activé peuvent disposer d'une période de conservation par défaut qui s'applique aux versions d'objet dont les paramètres de conservation ne sont pas définis lors de l'ingestion.	Oui.
La période de conservation peut-elle être modifiée ?	La date de conservation pour une version d'objet peut être augmentée mais jamais réduite.	La période de rétention du 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.
Quand les objets peuvent-ils être supprimés ?	Une version d'objet peut être supprimée après avoir atteint la date de conservation, en supposant que l'objet n'est pas en attente légale.	Un objet peut être supprimé après l'expiration de la période de conservation, en supposant que le compartiment n'est pas en conservation légale. Les objets peuvent être supprimés automatiquement ou manuellement.
La configuration du cycle de vie des compartiments est-elle prise en	Oui.	Non

Workflow pour le verrouillage d'objets S3

En tant qu'administrateur du grid, vous devez coordonner étroitement avec les utilisateurs des locataires pour assurer la protection des objets conformément aux exigences de conservation.

Le schéma des workflows représente les étapes générales d'utilisation du verrouillage d'objet S3. Ces étapes sont réalisées par l'administrateur du grid et les utilisateurs locataires.



Tâches d'administration du grid

Comme le montre le diagramme de workflow, un administrateur grid doit effectuer deux tâches générales avant que les locataires S3 ne puissent utiliser S3 Object Lock :

1. Créez au moins une règle ILM conforme et faites de cette règle la règle par défaut dans la politique ILM active.
2. Activez le paramètre global de verrouillage d'objet S3 pour l'ensemble du système StorageGRID.

Tâches des locataires

Une fois que le paramètre global de verrouillage d'objet S3 a été activé, les locataires peuvent effectuer les tâches suivantes :

1. Créez des compartiments dont le verrouillage d'objet S3 est activé.
2. Spécifiez les paramètres de conservation par défaut du compartiment, qui sont appliqués aux objets ajoutés au compartiment et qui ne définissent pas leurs propres paramètres de conservation.
3. Ajoutez des objets à ces compartiments et spécifiez les périodes de conservation au niveau de l'objet et les paramètres de conservation légale.
4. Si nécessaire, mettez à jour une période de conservation ou modifiez le paramètre de conservation légale d'un objet individuel.

Informations associées

- [Utilisez un compte de locataire](#)
- [Utilisation de S3](#)
- [Utilisez la conservation de compartiment par défaut avec le verrouillage d'objet S3](#)

Conditions requises pour le verrouillage d'objet S3

Vous devez connaître les exigences relatives à l'activation du paramètre global de verrouillage d'objet S3, les exigences de création de règles ILM et de règles ILM conformes, et les restrictions StorageGRID placées sur des compartiments et des objets qui utilisent le verrouillage d'objet S3.

Conditions requises pour l'utilisation du paramètre global de verrouillage d'objet S3

- Vous devez activer le paramètre global de verrouillage d'objet S3 à l'aide de Grid Manager ou de l'API Grid Management avant qu'un locataire S3 puisse créer un compartiment avec le verrouillage d'objet S3 activé.
- L'activation du paramètre global de verrouillage d'objet S3 permet à tous les comptes de locataires S3 de créer des compartiments avec le verrouillage d'objet S3 activé.
- Une fois que vous avez activé le paramètre global de verrouillage d'objet S3, vous ne pouvez pas désactiver le paramètre.
- Vous ne pouvez pas activer le verrouillage d'objet S3 global, à moins que la règle par défaut de la règle ILM active 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 de verrouillage de l'objet S3 est activé, vous ne pouvez pas créer de nouvelle règle ILM proposée ou activer une règle ILM existante, à moins que la règle par défaut de la règle ne soit conforme. Une fois le paramètre global S3 Object Lock activé, les pages ILM et ILM Rules indiquent les règles ILM compatibles.

Dans l'exemple suivant, la page des règles ILM répertorie trois règles compatibles avec des compartiments dont le verrouillage objet S3 est activé.

+ Create Clone Edit Remove			
Name	Compliant	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	✓	
Compliant Rule: EC for objects in bank-records bucket	✓		
2 copies 10 years, Archive forever			
2 Copies 2 Data Centers	✓		

Compliant Rule: EC for objects in bank-records bucket	
Description:	2+1 EC at one site
Ingest Behavior:	Balanced
Compliant:	Yes
Tenant Accounts:	Bank of ABC (94793396288150002349)
Bucket Name:	equals 'bank-records'
Reference Time:	Ingest Time

Exigences relatives aux règles ILM conformes

Si vous souhaitez activer le paramètre global de verrouillage d'objet S3, vous devez vous assurer que la règle par défaut de votre stratégie ILM active est conforme. Une règle conforme répond aux exigences des deux compartiments avec le verrouillage de l'objet S3 activé et les compartiments existants pour lesquels la conformité de l'ancienne génération est activée :

- Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
- Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
- Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
- Les copies d'objet ne peuvent pas être enregistrées sur les nœuds d'archivage.
- Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant **temps d'ingestion** comme heure de référence.
- Au moins une ligne des instructions de placement doit être ""permanente".

Par exemple, cette règle répond aux exigences des compartiments avec le verrouillage d'objet S3 activé. Il stocke deux copies d'objets répliquées de la durée d'ingestion (jour 0) à « permanente ». Les objets seront stockés sur les nœuds de stockage de deux data centers.

Compliant rule: 2 replicated copies at 2 sites	
Description:	2 replicated copies on Storage Nodes from Day 0 to Forever
Ingest Behavior:	Balanced
Compliant:	Yes
Tenant Accounts:	Bank of ABC (94793396288150002349)
Reference Time:	Ingest Time
Filtering Criteria:	Matches all objects.
Retention Diagram:	The diagram shows two horizontal bars representing retention periods for DC1 and DC2. Both bars start at 'Day 0' and extend to 'Forever'. DC1 is represented by a blue bar and DC2 by an orange bar. A vertical line marks the start at 'Day 0'.

Exigences relatives aux règles ILM actives et proposées

Lorsque le paramètre global S3 Object Lock est activé, les règles ILM actives et proposées peuvent inclure des règles conformes et non conformes.

- La règle par défaut de la politique ILM active ou proposée doit être conforme.
- Les règles non conformes s'appliquent uniquement aux objets dans les compartiments dont le verrouillage d'objet S3 n'est pas activé ou dont la fonctionnalité de conformité héritée n'est pas activée.
- Les règles conformes peuvent s'appliquer aux objets dans n'importe quel compartiment. Il n'est pas nécessaire d'activer le verrouillage objet S3 ou la conformité héritée.

Une politique ILM conforme peut inclure ces trois règles :

1. Règle de conformité qui crée des copies avec code d'effacement des objets dans un compartiment spécifique lorsque le verrouillage objet S3 est activé. Les copies EC sont stockées sur les nœuds de stockage du premier jour vers toujours.
2. Une règle non conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage pendant un an, puis déplace une copie d'objet vers les nœuds d'archivage et stocke cette copie indéfiniment. Cette règle s'applique uniquement aux compartiments dont le verrouillage d'objet S3 ou la conformité héritée n'est pas activée car elle stocke une seule copie d'objet à l'infini et utilise des nœuds d'archivage.
3. Règle par défaut conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage du jour 0 à l'infini. Cette règle s'applique à tout objet dans un compartiment qui n'a pas été filtré par les deux premières règles.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.

Dans cet exemple, le gestionnaire des locataires affiche un compartiment avec le verrouillage objet S3 activé.

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾						
☐	Name ▾	S3 Object Lock ⓘ ▾	Region ▾	Object Count ⓘ ▾	Space Used ⓘ ▾	Date Created ▾
☐	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un compartiment existant.
- Le contrôle de version de compartiment est requis avec le verrouillage d'objet S3. Lorsque le verrouillage

d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment.

- Une fois que vous avez créé un compartiment avec le verrouillage d'objet S3 activé, vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre la gestion des versions pour ce compartiment.
- Vous pouvez également configurer la conservation par défaut d'un compartiment. Lors du téléchargement d'une version d'objet, la conservation par défaut est appliquée à la version de l'objet. Vous pouvez remplacer la valeur par défaut du compartiment en spécifiant un mode de rétention et une date de conservation dans la demande de téléchargement d'une version d'objet.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments de cycle de vie des objets S3.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger la version d'un objet, l'application client S3 doit configurer la conservation par défaut du compartiment ou spécifier les paramètres de conservation dans chaque demande de téléchargement.
- Vous pouvez augmenter la valeur de conservation jusqu'à la date d'une version d'objet, mais vous ne pouvez jamais la diminuer.
- Si vous êtes averti d'une action légale ou d'une enquête réglementaire en attente, vous pouvez conserver les informations pertinentes en plaçant une mise en garde légale sur une version d'objet. Lorsqu'une version d'objet est soumise à une conservation légale, cet objet ne peut pas être supprimé de StorageGRID, même si elle a atteint sa date de conservation. Dès que la mise en attente légale est levée, la version de l'objet peut être supprimée si la date de conservation a été atteinte.
- Le verrouillage d'objet S3 requiert l'utilisation de compartiments avec version. 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 avec l'option de verrouillage d'objet S3 passe en trois étapes :

1. Entrée d'objet

- Lorsque vous ajoutez une version d'objet dans un compartiment lorsque le verrouillage objet S3 est activé, l'application client S3 peut utiliser les paramètres de conservation du compartiment par défaut ou spécifier des paramètres de conservation pour l'objet (conservation à la date, conservation légale ou les deux). StorageGRID génère ensuite les métadonnées de cet objet, qui incluent un identificateur d'objet unique (UUID) et la date et l'heure d'ingestion.
- Lors de l'ingestion d'une version d'objet avec paramètres de conservation, les données et les métadonnées S3 définies par l'utilisateur ne peuvent pas être modifiées.
- StorageGRID stocke les métadonnées objet indépendamment des données de l'objet. Elle conserve trois copies de toutes les métadonnées d'objet sur chaque site.

2. Rétention d'objet

- Plusieurs copies de l'objet sont stockées par StorageGRID. Le nombre et le type exacts de copies ainsi que les emplacements de stockage sont déterminés par les règles conformes de la politique ILM active.

3. Suppression d'objet

- Un objet peut être supprimé lorsque sa date de conservation est atteinte.
- Impossible de supprimer un objet en attente légale.

Informations associées

- [Utilisez un compte de locataire](#)
- [Utilisation de S3](#)
- [Comparaison du verrouillage d'objet S3 à la conformité existante](#)
- [Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3](#)
- [Examiner les journaux d'audit](#)
- [Utilisez la conservation de compartiment par défaut avec le verrouillage d'objet S3.](#)

Activez le verrouillage global des objets S3

Si un compte de locataire S3 doit respecter les exigences réglementaires lors de la sauvegarde des données d'objet, vous devez activer le verrouillage objet S3 pour l'intégralité de votre système StorageGRID. L'activation du paramètre de verrouillage d'objet S3 global permet aux locataires S3 de créer et de gérer des compartiments et des objets avec le verrouillage d'objet S3.

Ce dont vous avez besoin

- Vous disposez de l'autorisation d'accès racine.
- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous avez passé en revue le workflow de verrouillage d'objet S3 et vous devez comprendre les considérations à prendre en compte.
- La règle par défaut de la politique ILM active est conforme.
 - [Créez une règle ILM par défaut](#)
 - [Création d'une règle ILM](#)

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.



Si vous avez activé le paramètre de conformité globale à l'aide d'une version précédente de StorageGRID, le paramètre verrouillage objet S3 est activé dans StorageGRID 11.6. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants. Cependant, vous ne pouvez pas créer de compartiments conformes. Voir ["Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"](#).

Étapes

1. Sélectionnez **CONFIGURATION système verrouillage objet S3**.

La page Paramètres de verrouillage d'objet S3 s'affiche.

S3 Object Lock Settings

Enable S3 Object Lock for your entire StorageGRID system if S3 tenant accounts need to satisfy regulatory compliance requirements when saving object data. After this setting is enabled, it cannot be disabled.

S3 Object Lock

Before enabling S3 Object Lock, you must ensure that the default rule in the active ILM policy is compliant. A compliant rule satisfies the requirements of buckets with S3 Object Lock enabled.

- It must create at least two replicated object copies or one erasure-coded copy.
- These copies must exist on Storage Nodes for the entire duration of each line in the placement instructions.
- Object copies cannot be saved on Archive Nodes.
- At least one line of the placement instructions must start at day 0, using Ingest Time as the reference time.
- At least one line of the placement instructions must be "forever".

☐ Enable S3 Object Lock

Apply

Si vous avez activé le paramètre de conformité globale à l'aide d'une version précédente de StorageGRID, la page comprend la remarque suivante :

The S3 Object Lock setting replaces the legacy Compliance setting. When this setting is enabled, tenant users can create buckets with S3 Object Lock enabled. Tenants who previously created buckets for the legacy Compliance feature can manage their existing buckets, but can no longer create new buckets with legacy Compliance enabled. See [Managing objects with information lifecycle management](#) for information.

2. Sélectionnez **Activer le verrouillage d'objet S3**.

3. Sélectionnez **appliquer**.

Une boîte de dialogue de confirmation s'affiche et vous rappelle que vous ne pouvez pas désactiver le verrouillage d'objet S3 une fois qu'il est activé.

Info

Enable S3 Object Lock

Are you sure you want to enable S3 Object Lock for the grid? You cannot disable S3 Object Lock after it has been enabled.

Cancel

OK

4. Si vous êtes sûr de vouloir activer définitivement le verrouillage d'objet S3 pour l'ensemble du système, sélectionnez **OK**.

Lorsque vous sélectionnez **OK**:

- Si la règle par défaut de la politique ILM active est conforme, le verrouillage de l'objet S3 est 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, indiquant que vous devez créer et activer une nouvelle politique ILM incluant une règle conforme comme règle par défaut. Sélectionnez **OK**, créez une nouvelle stratégie proposée, simulez-la et activez-la.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

The default rule in the active ILM policy is not compliant.

OK

Une fois que vous avez terminé

Après avoir activé le paramètre global de verrouillage d'objet S3, vous devrez peut-être le faire [créer une règle par défaut](#) les données sont conformes et [Création d'une règle ILM](#) c'est-à-dire conforme. Une fois le paramètre activé, la règle ILM peut éventuellement inclure une règle par défaut conforme et une règle par défaut non compatible. Par exemple, vous pouvez utiliser une règle non conforme qui ne contient pas de filtres pour les objets dans les compartiments où le verrouillage d'objet S3 n'est pas activé.

Informations associées

- [Comparer le verrouillage d'objet S3 à la conformité existante](#)

Résolvez les erreurs de cohérence lors de la mise à jour de la configuration du verrouillage d'objet S3 ou de la conformité héritée

Si un site de data Center ou plusieurs nœuds de stockage sur un site deviennent indisponibles, les locataires S3 peuvent avoir à appliquer des modifications à la configuration de verrouillage d'objet S3 ou de conformité héritée.

Les locataires qui utilisent des compartiments avec le verrouillage d'objet S3 (ou la conformité héritée) peuvent modifier certains paramètres. Par exemple, un utilisateur locataire qui utilise le verrouillage objet S3 peut avoir à mettre une version d'objet en attente légale.

Lorsqu'un locataire met à jour les paramètres d'un compartiment S3 ou d'une version d'objet, StorageGRID tente immédiatement de mettre à jour les métadonnées du compartiment ou de l'objet dans la grille. Si le système ne peut pas mettre à jour les métadonnées car un site de data Center ou plusieurs nœuds de stockage ne sont pas disponibles, un message d'erreur s'affiche. Détails :

- Les utilisateurs de tenant Manager voient le message d'erreur suivant :

! Error

503: Service Unavailable

Unable to update compliance settings because the changes cannot be consistently applied on enough storage services. Contact your grid administrator for assistance.

OK

- Les utilisateurs de l'API de gestion des locataires et de l'API S3 reçoivent un code de réponse de 503 `Service Unavailable` avec un texte de message similaire.

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](#)
- [Utilisation de S3](#)
- [Récupérer et entretenir](#)

Exemples de règles et de règles ILM

Exemple 1 : règles et règles ILM pour le stockage objet

Vous pouvez utiliser les exemples de règles et de règle suivants comme point de départ pour définir une règle ILM afin de répondre à vos exigences de protection et de conservation des objets.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1, par exemple : copie des données d'objet dans deux data centers

Cet exemple de règle ILM copie les données d'objet vers les pools de stockage dans deux data centers.

Définition de règle	Exemple de valeur
Pools de stockage	Deux pools de stockage, chacun dans des data centers différents, nommés Storage Pool DC1 et Storage Pool DC2.
Nom de la règle	Deux copies pour les data centers
Heure de référence	Temps d'ingestion
Placement de contenu	Au jour 0, conservez deux copies répliquées à jamais : une dans Storage Pool DC1 et une dans Storage Pool DC2.

Règle ILM 2, par exemple 1 : profil de codage d'effacement avec mise en correspondance des compartiments

Cette 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
Profil de codage d'effacement	• Un pool de stockage répartis sur trois data centers (les 3 sites) • Utilisez le schéma de code d'effacement 6+3
Nom de la règle	EC pour les enregistrements financiers du compartiment S3
Heure de référence	Temps d'ingestion
Placement de contenu	Pour les objets du compartiment S3 appelés « enregistrements financiers », créez une copie avec code d'effacement dans le pool spécifié par le profil de code d'effacement. Conserver cette copie pour toujours.

Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

EC for S3 bucket finance-records

Reference Time

Ingest Time

Placements

Sort by start day

From day

0

store

forever

Add

Remove

Type

erasure coded

Location

All 3 sites (6 plus 3)

Copies

1

+

×

Retention Diagram

Refresh

Trigger

Day 0

Duration

Forever

Cancel Back Next

Règle ILM, par exemple 1

Le système StorageGRID vous permet de concevoir des règles ILM complexes et sophistiquées. Cependant, en pratique, la plupart des règles ILM sont simples.

Une règle ILM type pour une topologie multisite peut inclure des règles ILM telles que :

- Lors de l'ingestion, utilisez le code d'effacement 6+3 pour stocker tous les objets appartenant au compartiment S3 nommé `finance-records` sur trois data centers.
- Si un objet ne correspond pas à la première règle ILM, utilisez la règle ILM par défaut de la règle, deux copies deux Data Centers, pour stocker une copie de cet objet dans deux data centers, DC1 et DC2.

Exemple 2 : règles et règle ILM pour le filtrage de la taille des objets EC

Des exemples de règles et de règles ci-dessous vous permettent de définir une règle ILM qui s'applique par taille d'objet afin de répondre aux exigences EC recommandées.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1, par exemple 2 : utilise ce pour les objets de plus de 1 Mo

Cet exemple de règle ILM code des objets dont le nombre est supérieur à 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	EC uniquement les objets 1 Mo
Heure de référence	Temps d'ingestion
Filtrage avancé pour la taille de l'objet	Taille de l'objet (Mo) supérieure à 1
Placement de contenu	Créez une copie avec code d'effacement 2+1 sur trois sites

Règle ILM 2, par exemple 2 : deux copies répliquées

Cet exemple de règle ILM crée deux copies répliquées, sans filtrer par taille d'objet. Cette règle est la règle par défaut de la règle. Étant donné que la première règle filtre tous les objets de plus de 1 Mo, cette règle s'applique uniquement aux objets de 1 Mo ou plus.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Heure de référence	Temps d'ingestion
Filtrage avancé pour la taille de l'objet	Aucune
Placement de contenu	Créez deux copies répliquées et enregistrez-les dans deux data centers : DC1 et DC2

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.

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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](#)

Default	Rule Name	Tenant Account	Actions
	EC only objects > 1 MB	—	
✓	Two replicated copies	—	

[Cancel](#) [Save](#)

Exemple 3 : règles et règles ILM pour une meilleure protection des fichiers image

Vous pouvez utiliser les exemples de règles et de règles suivants pour vous assurer que les images de plus de 1 Mo sont codées par effacement et que les deux copies sont faites d'images plus petites.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1 par exemple 3 : utilisez EC pour les fichiers image de plus de 1 Mo

Cet exemple de règle ILM utilise un filtrage avancé pour code d'effacement de tous les fichiers image de plus de 1 Mo.



Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour des objets de moins de 200 Ko afin d'éviter toute surcharge liée à la gestion de fragments très petits codés d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	Fichiers image EC 1 Mo
Heure de référence	Temps d'ingestion
Filtrage avancé pour la taille de l'objet	Taille de l'objet (Mo) supérieure à 1.0
Filtrage avancé pour les métadonnées utilisateur	Le type de métadonnées utilisateur est égal à l'image
Placement de contenu	Créez une copie avec code d'effacement 2+1 sur trois sites

EC image files > 1 MB

Matches all of the following metadata:

Object Size (MB)greater than1+×

User Metadatatypeequalsimage+×

+×

Étant donné que cette règle est configurée comme première règle de la règle, l'instruction de placement de code d'effacement s'applique uniquement aux images supérieures à 1 Mo.

Règle ILM 2, par exemple 3 : création de 2 copies répliquées pour tous les fichiers d'images restants

Cet exemple de règle ILM utilise un filtrage avancé pour spécifier la réplication de fichiers d'images plus petits. Comme la première règle de la stratégie a déjà mis en correspondance des fichiers d'image de plus de 1 Mo, cette règle s'applique aux fichiers d'image de 1 Mo ou moins.

Définition de règle	Exemple de valeur
Nom de la règle	2 copies pour les fichiers image
Heure de référence	Temps d'ingestion
Filtrage avancé pour les métadonnées utilisateur	Le type de métadonnées utilisateur est égal aux fichiers image

Définition de règle	Exemple de valeur
Placement de contenu	Créez deux copies répliquées dans deux pools de stockage

Règle ILM, par exemple 3 : meilleure protection des fichiers image

Cet exemple de règle ILM comprend trois règles :

- La première règle code tous les fichiers image de plus de 1 Mo.
- La deuxième règle crée deux copies de tous les fichiers d'image restants (c'est-à-dire les images de 1 Mo ou plus).
- La règle par défaut s'applique à tous les objets restants (c'est-à-dire tous les fichiers non images).

Exemple 4 : règles et règles ILM pour les objets avec version S3

Si la gestion des versions est activée pour un compartiment S3, vous pouvez gérer les versions d'objet non actuelles en incluant des règles de votre stratégie ILM qui utilisent **Noncurrent Time** comme temps de référence.

Comme le montre cet exemple, vous pouvez contrôler la quantité de stockage utilisée par les objets avec version à l'aide d'instructions de placement différentes pour les versions d'objets non actuelles.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.



Si vous créez des règles ILM pour gérer les versions d'objets non actuelles, notez que vous devez connaître l'UUID ou l'identifiant CBID de la version de l'objet pour simuler la règle. Pour trouver l'UUID et le CBID d'un objet, utilisez recherche de métadonnées objet pendant que l'objet est toujours à jour. Voir [Vérification d'une règle ILM avec la recherche de métadonnées d'objet](#).

Informations associées

- [Comment supprimer les objets](#)

Règle ILM 1, par exemple 4 : trois copies économisées sur 10 ans

Cet exemple de règle ILM stocke une copie de chaque objet dans trois data centers 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 situé dans des data centers différents, nommés DC1, DC2 et DC3.
Nom de la règle	Trois copies dix ans

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placement de contenu	Au jour 0, conservez trois copies répliquées pendant 10 ans (3,652 jours), une pour DC1, une pour DC2 et une pour DC3. 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. Cette règle utilise l'option **Noncurrent Time** pour l'heure de référence.

Dans cet exemple, seules deux copies des versions non actuelles sont stockées, et ces copies seront stockées pendant deux ans.

Définition de règle	Exemple de valeur
Pools de stockage	Deux pools de stockage, chacun situé dans des data centers différents, nommés DC1 et DC2.
Nom de la règle	Versions non actuelles : deux copies deux ans
Heure de référence	Heure non actuelle
Placement de contenu	Le jour 0 relatif à l'heure non actuelle (c'est-à-dire à partir du jour où la version de l'objet devient la version non actuelle), conservez deux copies répliquées des versions de l'objet non courant pendant 2 ans (730 jours), une dans DC1 et une dans DC2. À la fin de 2 ans, supprimer les versions non actuelles.

Règle ILM, par exemple 4 : objets avec version S3

Si vous souhaitez gérer les anciennes versions d'un objet différemment de la version actuelle, les règles qui utilisent **Noncurrent Time** comme temps de référence doivent apparaître dans la stratégie ILM avant que les règles s'appliquent à la version actuelle de l'objet.

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 d'heure non actuelles doivent apparaître dans la stratégie avant que les règles s'appliquent à la version actuelle de l'objet. Dans le cas contraire, les versions d'objet non actuelles ne seront jamais mises en correspondance par la règle temps non actuel.

- Lors de leur entrée, créez trois copies répliquées et stockez une copie dans chacun des trois data centers. Conservez les copies de la version actuelle de l'objet pendant 10 ans.

Lorsque vous simulez l'exemple de stratégie, vous vous attendez à ce que les objets test soient évalués comme suit :

- Toutes les versions d'objet non courantes seront mises en correspondance par la première règle. Si une version d'objet non actuelle a plus de 2 ans, elle est supprimée définitivement par ILM (toutes les copies de la version non actuelle sont supprimées de la grille).



Pour simuler des versions d'objet non actuelles, vous devez utiliser l'UUID ou le CBID de cette version. Bien que l'objet soit encore à jour, vous pouvez utiliser la recherche de métadonnées d'objet pour trouver son UUID et son CBID.

- La version actuelle de l'objet sera comparée à la seconde règle. Lorsque la version actuelle de l'objet a été stockée pendant 10 ans, le processus ILM ajoute un marqueur de suppression comme version actuelle de l'objet, et il 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 au DC3 est purgée et les deux copies au DC1 et DC2 sont conservées pendant deux années supplémentaires.

Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict

Vous pouvez utiliser un filtre d'emplacement et un comportement d'ingestion strict dans une règle pour empêcher la sauvegarde des objets dans un emplacement de data Center spécifique.

Dans cet exemple, un locataire basé à Paris ne veut pas stocker certains objets en dehors de l'UE en raison de préoccupations réglementaires. Les autres objets, et notamment tous les objets des autres comptes locataires, peuvent être stockés dans le data Center de Paris ou dans le data Center des États-Unis.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Informations associées

- [Options de protection des données pour l'ingestion](#)
- [Étape 3 sur 3 : définir le comportement d'entrée](#)

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 de locataire	Locataire Paris
Filtrage avancé	La contrainte d'emplacement est égale à eu-West-3
Pools de stockage	DC1 (Paris)
Nom de la règle	Ingestion stricte pour le data Center de Paris
Heure de référence	Temps d'ingestion
Placement de contenu	Au premier jour, conservez deux copies répliquées à jamais dans DC1 (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

Description: Strict ingest to guarantee Paris data center

Ingest Behavior: Strict

Tenant Account: Paris tenant (25580610012441844135)

Reference Time: Ingest Time

Filtering Criteria:

Matches all of the following metadata:

System Metadata
Location Constraint (S3 only)
equals
eu-west-3

Retention Diagram:

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, des copies intermédiaires sont stockées à tout 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 de locataire	Ignorer
Filtrage avancé	<i>Non spécifié</i>
Pools de stockage	DC1 (Paris) et DC2 (Etats-Unis)
Nom de la règle	2 copies 2 data centers
Heure de référence	Temps d'ingestion
Placement de contenu	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. Effectuez des copies provisoires à tout emplacement disponible si l'instruction de placement ne peut pas être satisfaite.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Example policy for Strict ingest

Reason for change

Do not store certain objects for Paris tenant in US

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

Default	Rule Name	Tenant Account	Actions
	Strict ingest to guarantee Paris data center 	Paris tenant (25580610012441844135)	✕
✓	2 Copies 2 Data Centers 	Ignore	✕

Cancel

Save

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 Paris ne sont pas disponibles, l'entrée échoue.
- Tous les autres objets sont mis en correspondance par la deuxième règle, y compris les objets appartenant au locataire Paris et dont la région du compartiment S3 n'est pas définie sur eu-West-3. Une copie de chaque objet est enregistrée dans chaque data Center. Cependant, la seconde règle utilise une ingestion équilibrée, si un data Center n'est plus disponible, deux copies intermédiaires sont enregistrées à tout emplacement disponible.

Exemple 6 : modification d'une règle ILM

Vous devrez peut-être créer et activer une nouvelle règle ILM si la protection des données a changé ou si vous ajoutez de nouveaux sites.

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 lors d'une extension et la politique ILM active doit être révisée pour stocker les données sur le nouveau site.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

La modification d'une règle ILM affecte-t-elle 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.

Les types de modifications de règles ILM susceptibles d'affecter temporairement les performances de StorageGRID sont les suivants :

- Application d'un profil de code d'effacement différent aux objets avec code d'effacement existants



StorageGRID considère que chaque profil de code d'effacement est 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).

Informations associées

[Création d'une règle ILM](#)

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.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

[+ Create Proposed Policy](#) [Clone](#) [Edit](#) [Remove](#)

Policy Name	Policy State	Start Date	End Date
☒ Data Protection for Two Sites	Active	2020-06-10 16:42:09 MDT	
☐ Baseline 2 Copies Policy	Historical	2020-06-09 21:48:34 MDT	2020-06-10 16:42:09 MDT

Viewing Active Policy - Data Protection for Two Sites

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Two Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A 🔗		Tenant A (49752734300032812036)
Two-Site Replication for Other Tenants 🔗	✓	Ignore

[Simulate](#) [Activate](#)

Dans cette politique ILM, les objets appartenant au locataire A sont protégés par un code d'effacement 2+1 sur un seul site, tandis que les objets de tous les autres locataires sont protégés sur deux sites à l'aide de la réplication à 2 copies.



La première règle de cet exemple utilise un filtre avancé pour s'assurer que le codage d'effacement n'est pas utilisé pour les petits objets. Tout objet du locataire A dont la taille est inférieure à 1 Mo sera protégé par la deuxième règle qui utilise la réplication.

Règle 1 : code d'effacement sur un site pour le locataire A

Définition de règle	Exemple de valeur
Nom de la règle	Code d'effacement sur un site pour le locataire A
Compte de locataire	Locataire A
Pool de stockage	Data Center 1
Placement de contenu	Code d'effacement 2+1 dans le data Center 1, contre une date du 0 au Forever

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	Data Center 1 et Data Center 2

Définition de règle	Exemple de valeur
Placement de contenu	Deux copies répliquées du jour 0 à jamais : une copie dans le data Center 1 et une autre dans le data Center 2.

Politique ILM proposée, par exemple 6 : protection des données sur trois sites

Dans cet exemple, la politique ILM est mise à jour 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 Data Center 3 et un pool de stockage contenant les trois sites (différent du pool de stockage par défaut de tous les nœuds de stockage). L'administrateur a ensuite créé deux nouvelles règles ILM et une nouvelle règle ILM, conçue pour protéger les données des trois sites.

Viewing Proposed Policy - Data Protection for Three Sites

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Three Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Three-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Three-Site Replication for Other Tenants	✓	Ignore

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	Les 3 data centers (comprend le data Center 1, le data Center 2 et le data Center 3)
Placement de contenu	Dans les 3 data centers, le code d'effacement 2+1 n'a jamais été aussi utilisé

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	Data Center 1, Data Center 2 et Data Center 3
Placement de contenu	Trois copies répliquées depuis le jour 0 pour toujours : une copie dans le data Center 1, une copie dans le data Center 2 et une copie dans le data Center 3.

Activation de la politique ILM proposée, par exemple 6

Lorsque vous activez une nouvelle règle ILM, les objets existants peuvent être déplacés vers de nouveaux emplacements ou de nouvelles copies d'objet peuvent être créées pour des objets existants, en fonction des instructions de placement fournies dans toutes les règles mises à jour ou nouvelles.



Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Que se passe-t-il en cas de modification des instructions de code d'effacement

Dans cet exemple, les objets appartenant à la politique ILM actuellement active sont protégés à l'aide du code d'effacement 2+1 au data Center 1. Dans la nouvelle politique ILM proposée, les objets appartenant au locataire A seront protégés à l'aide du code d'effacement 2+1 dans les data centers 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. Chacun de ces trois fragments est ensuite stocké dans un data Center différent.
- Les objets existants appartenant au locataire A sont réévalués au cours du processus d'analyse ILM en cours. Les instructions de placement de ILM utilisent un nouveau profil de code d'effacement, ce qui crée et distribue des fragments avec code d'effacement dans les trois data centers.



Les fragments 2+1 existants dans le Data Center 1 ne sont pas réutilisés. StorageGRID considère que chaque profil de code d'effacement est 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, dans la politique ILM actuellement active, les objets appartenant à d'autres locataires sont protégés à l'aide de deux copies répliquées dans les pools de stockage des data centers 1 et 2. Dans la nouvelle politique ILM proposée, les objets appartenant à d'autres locataires sont protégés à l'aide de trois copies répliquées dans les pools de stockage des data centers 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 analyse un nouvel objet, StorageGRID crée trois copies et sauvegarde une copie dans chaque data Center.
- Les objets existants appartenant à ces autres locataires sont réévalués en cours d'analyse ILM. Les copies d'objets existantes au niveau du data Center 1 et du data Center 2 continuent de satisfaire les exigences de réplication de la nouvelle règle ILM, StorageGRID ne doit créer qu'une nouvelle copie de l'objet pour le data Center 3.

Impact sur les performances de l'activation de cette stratégie

Lorsque la politique ILM proposée dans cet exemple est activée, les performances globales de ce système StorageGRID sont temporairement affectées. Des niveaux supérieurs aux niveaux normaux des ressources de grid seront nécessaires pour créer de nouveaux fragments avec code d'effacement pour les objets existants du locataire A, ainsi que de nouvelles copies répliquées dans le data Center 3 pour les objets existants d'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 de temps d'ingestion dans n'importe quelle règle qui pourrait modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps de transfert sur une valeur supérieure ou égale à la durée approximative de mise en œuvre de la nouvelle stratégie pour garantir que les objets existants ne sont pas déplacés inutilement.



Contactez le support technique si vous avez besoin de ralentir ou d'augmenter le taux de traitement des objets après une modification de la règle ILM.

Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3

Vous pouvez utiliser le compartiment S3, les règles ILM et la règle ILM dans cet exemple à partir d'un point de départ lors de la définition d'une règle ILM afin de répondre aux exigences de protection et de conservation des objets dans des compartiments où le verrouillage d'objet S3 est activé.



Si vous avez utilisé la fonctionnalité de conformité héritée dans les versions précédentes de StorageGRID, vous pouvez également utiliser cet exemple pour gérer les compartiments existants pour lesquels la fonctionnalité de conformité héritée est activée.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Informations associées

- [Gestion des objets avec le verrouillage d'objets S3](#)
- [Création d'une règle ILM](#)

Exemple de compartiment et d'objets pour le verrouillage d'objet S3

Dans cet exemple, un compte de locataire S3 nommé Bank of ABC a utilisé le gestionnaire de locataires pour créer un compartiment avec le verrouillage objet S3 activé pour stocker les enregistrements bancaires stratégiques.

Définition du compartiment	Exemple de valeur
Nom du compte du locataire	Banque d'ABC
Nom du compartiment	les registres bancaires
Région du godet	us-east-1 (par défaut)

Buckets

Create buckets and manage bucket settings.

1 bucket Create bucket

Actions ▾

☐	Name ▾	S3 Object Lock ? ▾	Region ▾	Object Count ? ▾	Space Used ? ▾	Date Created ▾
☐	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

Chaque objet et version d'objet ajoutés au compartiment des enregistrements bancaires utilise les valeurs suivantes pour `retain-until-date` et `legal hold` paramètres.

Paramètre pour chaque objet	Exemple de valeur
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 décembre 2030) Chaque version d'objet a sa propre version <code>retain-until-date</code> réglage. Ce réglage peut être augmenté, mais pas diminué.
<code>legal hold</code>	"OFF" (Pas en vigueur) Une mise en garde légale peut être placée ou levée sur n'importe quelle version d'objet à tout moment pendant la période de conservation. Si un objet est en attente légale, il ne peut pas être supprimé, même si <code>retain-until-date</code> a été atteint.

Règle ILM 1 pour exemple de verrouillage d'objet S3 : profil de codage d'effacement avec mise en correspondance de compartiment

Cet exemple de règle ILM s'applique uniquement au compte de locataire S3 nommé Bank of ABC. Il correspond à n'importe quel objet du `bank-records`. Les compartiments utilisent ensuite le code d'effacement pour stocker l'objet sur les nœuds de stockage sur trois sites de data Center à l'aide d'un profil de code d'effacement 6+3. Cette règle répond aux exigences des compartiments avec le verrouillage objet S3 activé : une copie avec code d'effacement est conservée sur les nœuds de stockage du jour 0 à l'infini, en utilisant l'heure de récupération comme heure de référence.

Définition de règle	Exemple de valeur
Nom de la règle	Règle conforme : objets EC dans le compartiment de documents bancaires - Banque d'ABC
Compte de locataire	Banque d'ABC
Nom du compartiment	bank-records
Filtrage 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.

Create ILM Rule Step 1 of 3: Define Basics

Name

Compliant Rule: EC objects in bank-records bucket - Bank of ABC

Description

Uses 6+3 EC across 3 sites

Tenant Accounts (optional)

Bank of ABC (20770793906808351043) x

Bucket Name

equals

bank-records

Advanced filtering... (0 defined)

Cancel

Next

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	À partir du jour 0 magasin pour toujours
Profil de codage d'effacement	- Créez une copie avec code d'effacement sur les nœuds de stockage de trois sites de data Center - Utilise le schéma de code d'effacement 6+3

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Compliant Rule: EC objects in bank-record bucket - Bank of ABC

Reference Time
Ingest Time

Placements
Sort by start day

From day 0 store forever
Add Remove

Type erasure coded Location Three Data Centers (6 plus 3) Copies 1
+ x

Retention Diagram
Refresh

Trigger
Day 0
Three Data Centers (6 plus 3)
Duration
Forever

Cancel Back Save

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'applique uniquement aux compartiments qui n'ont pas le verrouillage d'objet S3 (ou la fonctionnalité de conformité héritée) activé.
Filtrage avancé	Non spécifié

Name	Non-Compliant Rule: Use Cloud Storage Pool	
Description	DC1 and 2 for 1 year then move to CSP	
Tenant Accounts (optional) ?	Select tenant accounts or enter tenant IDs	
Bucket Name	matches all ▼	Value
Advanced filtering... (0 defined)		

Cancel

Next

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 deux centres de données
Compte de locataire	Non spécifié
Nom du compartiment	Non spécifié
Filtrage avancé	Non spécifié

Name	Compliant Rule: Two Copies Two Data Centers
Description	2 copies on SNs from day 1 to forever, reference time is ingest
Tenant Accounts (optional)	Select tenant accounts or enter tenant IDs
Bucket Name	matches all Value

[Advanced filtering...](#) (0 defined)

Cancel Next

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.

Compliant Rule: Two Copies Two Data Centers

Reference Time: Ingest Time

Placements Sort by start day

From day: 0 store: forever Add Remove

Type: replicated Location: Data Center 1 Data Center 2 Add Pool Copies: 2 + -

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

The diagram illustrates the retention policy for two data centers. A vertical line marks 'Day 0' as the 'Trigger' point. For 'Data Center 1', a blue bar represents the retention duration, which extends to the right towards 'Forever'. Similarly, for 'Data Center 2', an orange bar represents the retention duration, also extending to the right towards 'Forever'. The x-axis is labeled 'Duration' and the y-axis is labeled 'Forever'.

Exemple de règle ILM conforme pour l'exemple de verrouillage d'objet S3

Pour créer une règle ILM protégeant efficacement tous les objets de votre système, y compris ceux des compartiments avec le verrouillage objet S3 activé, vous devez sélectionner des règles ILM qui répondent aux besoins de stockage de tous les objets. Vous devez ensuite simuler et activer la règle proposée.

Ajouter des règles à la règle

Dans cet exemple, la politique ILM inclut trois règles ILM, dans l'ordre suivant :

1. Règle conforme qui utilise le code d'effacement pour protéger les objets de plus de 1 Mo dans un

compartiment spécifique avec le verrouillage objet S3 activé. Les objets sont stockés sur les nœuds de stockage du premier jour vers toujours.

2. Une règle non conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage pendant un an, puis déplace une copie d'objet vers un pool de stockage cloud à tout moment. Cette règle ne s'applique pas aux compartiments avec le verrouillage d'objet S3 activé car elle utilise un pool de stockage cloud.
3. La règle de conformité par défaut qui crée deux copies d'objets répliquées sur les nœuds de stockage du jour 0 à l'infini.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name Compliant ILM policy for S3 Object Lock example

Reason for change Example policy

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 (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC 	✓	Bank of ABC (90767802913525281639)	✗
	Non-Compliant Rule: Use Cloud Storage Pool 		Ignore	✗
✓	Default Compliant Rule: Two Copies Two Data Centers 	✓	Ignore	✗

Cancel

Save

Simuler la règle proposée

Une fois que vous avez ajouté des règles dans la stratégie proposée, choisi une règle conforme par défaut et arrangé les autres règles, vous devez simuler la règle en testant les objets à partir du compartiment avec le verrouillage d'objet S3 activé et à partir d'autres compartiments. Par exemple, lorsque vous simulez l'exemple de règle, vous attendez à ce que les objets test soient évalués comme suit :

- La première règle correspond uniquement aux objets de test supérieurs à 1 Mo dans les banques d'enregistrements du compartiment pour le locataire Bank of ABC.
- La deuxième règle fait correspondre tous les objets de tous les compartiments non conformes pour tous les autres comptes de tenant.
- La règle par défaut correspond à ces objets :
 - Objets de 1 Mo ou plus petits dans les banques d'enregistrements du compartiment pour le locataire Banque d'ABC.
 - Objets dans tout autre compartiment pour lequel le verrouillage objet S3 est activé pour tous les autres comptes locataires.

Activer la règle

Si vous êtes pleinement satisfait de la nouvelle règle assurant la protection des données d'objet comme prévu, vous pouvez l'activer.

Durcissement du système

Durcissement du système : vue d'ensemble

Le renforcement des systèmes consiste à éliminer autant de risques que possible pour la sécurité d'un système StorageGRID.

Ce document présente les directives de renforcement propres à StorageGRID. Ces directives constituent un complément aux meilleures pratiques standard du secteur en matière de renforcement des systèmes. Par exemple, ces instructions partent du principe que vous utilisez des mots de passe forts pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur les certificats, le cas échéant.

Lors de l'installation et de la configuration de StorageGRID, ces instructions vous aideront à répondre aux objectifs de sécurité que vous avez définis pour la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

StorageGRID suit la politique de gestion des vulnérabilités de *NetApp*. Toutes les vulnérabilités signalées sont vérifiées et traitées selon le processus de réponse aux incidents de sécurité.

Considérations générales relatives au renforcement des systèmes StorageGRID

Lors du renforcement d'un système StorageGRID, vous devez prendre en compte les éléments suivants :

- Parmi les trois réseaux StorageGRID que vous avez mis en place, lesquels ? Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau Admin, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- Type de plateforme utilisé pour les nœuds individuels du système StorageGRID. Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme dispose de son propre ensemble de meilleures pratiques en matière de renforcement.
- Fiabilité des comptes locataires. Si vous êtes un fournisseur de services avec des comptes de locataires non fiables, vous vous interrogez différemment que si vous utilisez uniquement des locataires internes fiables.
- Les exigences et conventions de sécurité sont respectées par votre entreprise. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Informations associées

["Stratégie de gestion des vulnérabilités"](#)

Directives de renforcement des mises à niveau logicielles

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous protéger contre les attaques.

Mises à niveau du logiciel StorageGRID

Dans la mesure du possible, vous devez mettre à niveau le logiciel StorageGRID vers la version principale la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire le temps d'activation des vulnérabilités connues et de réduire la surface d'attaque globale. Les dernières versions d'StorageGRID incluent en outre souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

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 la page de téléchargement du logiciel StorageGRID. Pour obtenir des instructions détaillées sur la mise à niveau du logiciel StorageGRID, reportez-vous aux instructions de mise à niveau de StorageGRID. Pour obtenir des instructions sur l'application d'un correctif, reportez-vous aux instructions de récupération et de maintenance.

Mises à niveau vers des services externes

Les services externes peuvent comporter des vulnérabilités qui affectent indirectement StorageGRID. Vous devez vous assurer que les services dont dépend StorageGRID sont tenus à jour. Ces services incluent : LDAP, KMS (ou serveur KMIP), DNS et NTP.

Utilisez la matrice d'interopérabilité NetApp pour obtenir la liste des versions prises en charge.

Mises à niveau vers les hyperviseurs

Si vos nœuds StorageGRID s'exécutent sur VMware ou sur un autre hyperviseur, vous devez vous assurer que le logiciel et le firmware de l'hyperviseur sont à jour.

Utilisez la matrice d'interopérabilité NetApp pour obtenir la liste des versions prises en charge.

Mise à niveau vers des nœuds Linux

Si vos nœuds StorageGRID utilisent des plates-formes hôtes Linux, vous devez vous assurer que les mises à jour de sécurité et de noyau sont appliquées au système d'exploitation hôte. En outre, vous devez appliquer des mises à jour de micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Utilisez la matrice d'interopérabilité NetApp pour obtenir la liste des versions prises en charge.

Informations associées

["Téléchargement NetApp : StorageGRID"](#)

[Mise à niveau du logiciel](#)

[Récupérer et entretenir](#)

["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.

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. Consultez la liste des ports internes dans le guide d'installation de votre plate-forme.
- 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. Consultez la liste des ports internes dans le guide d'installation de votre plate-forme.
- Acceptez le trafic client entrant uniquement sur les terminaux configurés explicitement. Voir [Gestion des réseaux clients non fiables](#).

Informations associées

[Instructions de mise en réseau](#)

[Primaire de grille](#)

[Administrer StorageGRID](#)

[Installez Red Hat Enterprise Linux ou CentOS](#)

Instructions de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud dispose de ses propres pratiques de renforcement.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez examiner les configurations de pare-feu externes et les modifier afin que le trafic soit accepté uniquement à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

StorageGRID utilise un pare-feu interne géré automatiquement. Bien que ce pare-feu interne offre une couche supplémentaire de protection contre certaines menaces courantes, il ne supprime pas la nécessité d'un pare-feu externe.

Pour obtenir la liste de tous les ports internes et externes utilisés par StorageGRID, reportez-vous au guide d'installation de votre plate-forme.

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 partez pas du principe de protection de l'hyperviseur pour empêcher les programmes malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le programme malveillant existent tous deux 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.

Désactiver les services inutilisés

Pour tous les nœuds StorageGRID, désactivez ou bloquez l'accès aux services non utilisés. Par exemple, si vous n'avez pas l'intention de configurer l'accès du client aux partages d'audit pour CIFS ou NFS, bloquez ou désactivez l'accès à ces services.

Protéger les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID via le réseau lors de l'installation des nœuds. Les nœuds ne sont pas entièrement sécurisés tant qu'ils n'ont pas rejoint la grille.

Instructions pour les nœuds d'administration

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un 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 disposez de locataires non approuvés, ne leur autorisez pas à accéder directement 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 plus de contrôle sur les communications AutoSupport depuis les nœuds d'administration vers la prise en charge de NetApp. Reportez-vous aux étapes de création d'un proxy d'administration dans les instructions d'administration de StorageGRID.
- 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 d'administration de StorageGRID.

Consignes relatives aux nœuds de stockage

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Suivez ces instructions pour sécuriser les nœuds de stockage dans votre système StorageGRID.

- N'autorisez pas les clients non approuvés à se connecter directement aux nœuds de stockage. Utilisez un point de terminaison d'équilibrage de charge fourni par un nœud de passerelle ou un équilibreur de charge tiers.
- N'activez pas les services sortants pour les locataires non fiables. 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'autorise pas l'utilisation des services de plateforme. Reportez-vous aux étapes de création d'un compte de locataire dans les instructions d'administration de StorageGRID.
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour plus de contrôle sur les pools de stockage cloud et les communications des services de plateforme depuis les nœuds de stockage vers les services externes. Reportez-vous aux étapes de création d'un proxy de stockage dans les instructions d'administration de StorageGRID.
- Vous pouvez également vous connecter à des services externes à l'aide du réseau client. Sélectionnez ensuite **CONFIGURATION réseau réseaux client non fiables** et indiquez que le réseau client sur le nœud de stockage n'est pas fiable. Le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais il continue à autoriser les requêtes sortantes pour les services de plate-forme.

Instructions pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de la charge facultative que les applications client peuvent utiliser pour se connecter à StorageGRID. Pour sécuriser tous les nœuds de passerelle de votre système StorageGRID, procédez comme suit :

- Configurez et utilisez des terminaux d'équilibrage de charge au lieu d'utiliser le service CLB sur les nœuds de passerelle. Voir les étapes de gestion de l'équilibrage de charge dans les instructions d'administration de StorageGRID.



Le service CLB est obsolète.

- Utilisez un équilibreur de charge tiers entre le client et le nœud de passerelle ou les nœuds de stockage pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut, éventuellement, être configuré de manière à passer par un terminal interne d'équilibrage de la charge ou être directement envoyé aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, les clients peuvent éventuellement se connecter via le réseau client. Sélectionnez ensuite **CONFIGURATION réseau réseaux client non fiables** et indiquez que le réseau client sur le nœud passerelle n'est pas fiable. Le nœud passerelle accepte uniquement le trafic entrant sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge.

Consignes pour les nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour une utilisation dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. Les autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds de passerelle. Vous pouvez associer des nœuds d'appliance à des nœuds basés sur logiciel ou déployer des grilles 100 % appliance entièrement conçues.

Pour sécuriser les nœuds d'appliance matérielle de votre système StorageGRID, procédez comme suit :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non fiables d'accéder à SANtricity System Manager sur le réseau.
- Si l'appliance est équipée d'un contrôleur de gestion de la carte mère (BMC), notez que le port de gestion du BMC permet un accès matériel de faible niveau. Connectez le port de gestion BMC uniquement à un réseau de gestion interne sécurisé, fiable et. Si aucun réseau de ce type n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué, à moins qu'une connexion BMC ne soit demandée par le support technique.
- Si l'appliance prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme IPMI (Intelligent Platform Management interface), bloquez le trafic non fiable sur le port 623.
- Si le contrôleur de stockage de l'appliance inclut des disques FDE ou FIPS et que la fonction de sécurité des disques est activée, utilisez SANtricity pour configurer les clés de sécurité des disques.
- Pour les appliances sans disques FDE ou FIPS, activez le chiffrement de nœud à l'aide d'un serveur de gestion des clés (KMS).

Consultez les instructions d'installation et de maintenance de votre appliance matérielle StorageGRID.

Informations associées

- [Installez Red Hat Enterprise Linux ou CentOS](#)
- [Installez Ubuntu ou Debian](#)
- [Installez VMware](#)
- [Administrer StorageGRID](#)
- [Utilisez un compte de locataire](#)

- [Appareils de services SG100 et SG1000](#)
- [Appliances de stockage SG5600](#)
- [Appliances de stockage SG5700](#)
- [Dispositifs de stockage SG6000](#)

Consignes de renforcement des certificats de serveur

Vous devez remplacer les certificats par défaut créés lors de l'installation par vos propres certificats personnalisés.

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web StorageGRID n'est pas conforme à leurs politiques de sécurité de l'information. Sur les systèmes de production, vous devez installer un certificat numérique signé par une autorité de certification pour l'authentification de StorageGRID.

Plus précisément, vous devez utiliser des certificats de serveur personnalisés au lieu de ces certificats par défaut :

- **Certificat d'interface de gestion** : utilisé pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management.
- **Certificat API S3 et Swift** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications client S3 et Swift utilisent pour charger et télécharger des données d'objet.



StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer les certificats d'équilibreur de charge, reportez-vous aux étapes de configuration des nœuds finaux d'équilibreur de charge dans les instructions d'administration de StorageGRID.

Lorsque vous utilisez des certificats de serveur personnalisés, suivez les instructions suivantes :

- Les certificats doivent avoir un *subjectAltName* correspondant aux entrées DNS de StorageGRID. Pour plus de détails, reportez-vous à la section 4.2.1.6, «sous-objet autre nom», dans ["RFC 5280 : certificat PKIX et profil CRL"](#).
- Si possible, évitez d'utiliser des certificats génériques. Une exception à cette directive est le certificat d'un terminal de type hébergé virtuel S3. Il requiert l'utilisation d'un caractère générique si les noms de compartiment ne sont pas connus à l'avance.
- Lorsque vous devez utiliser des caractères génériques dans les certificats, vous devez prendre des mesures supplémentaires pour réduire les risques. Utilisez un motif générique comme `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour les autres applications. Ce modèle fonctionne également avec l'accès S3 de type chemin d'accès, comme `dc1-s1.s3.example.com/mybucket`.
- Définissez les délais d'expiration du certificat sur court (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

En outre, les clients doivent utiliser un contrôle strict du nom d'hôte lors de la communication avec StorageGRID.

Autres directives de durcissement

Outre les directives de renforcement des réseaux et nœuds StorageGRID, vous devez suivre les instructions de renforcement correspondant à d'autres domaines du système StorageGRID.

Journaux et messages d'audit

Protégez toujours les journaux StorageGRID et la sortie des messages d'audit de manière sécurisée. Les journaux et les messages d'audit StorageGRID fournissent des informations précieuses du point de vue du support et de la disponibilité du système. En outre, les informations figurant dans les journaux StorageGRID et dans les résultats des messages d'audit sont généralement sensibles.

Configurez StorageGRID pour envoyer des événements de sécurité à un serveur syslog externe. Si vous utilisez syslog export, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Pour plus d'informations sur les journaux StorageGRID, reportez-vous aux instructions de surveillance et de dépannage. Pour plus d'informations sur les messages d'audit StorageGRID, reportez-vous aux instructions relatives aux messages d'audit.

NetApp AutoSupport

La fonction AutoSupport de StorageGRID vous permet de surveiller de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque StorageGRID est configuré pour la première fois.

La fonction AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes sur le système StorageGRID.

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison de la nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.

Vous pouvez également configurer un proxy d'administration pour plus de contrôle sur les communications AutoSupport depuis les nœuds d'administration vers le support technique de NetApp. Reportez-vous aux étapes de création d'un proxy d'administration dans les instructions d'administration de StorageGRID.

Partage de ressources interorigine (CORS)

Vous pouvez configurer le partage de ressources inter-origine (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et les objets de ce compartiment soient accessibles aux applications Web dans d'autres domaines. En général, n'activez pas le CORS à moins qu'il ne soit nécessaire. Si CORS est requis, limitez-le aux origines de confiance.

Consultez les étapes de configuration du partage de ressources d'origine croisée (CORS) dans les instructions d'utilisation des comptes de tenant.

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.

Informations associées

[Surveiller et résoudre les problèmes](#)

[Examiner les journaux d'audit](#)

[Utilisez le compte du locataire](#)

[Administrer StorageGRID](#)

Configurez FabricPool

Configurer StorageGRID pour FabricPool : présentation

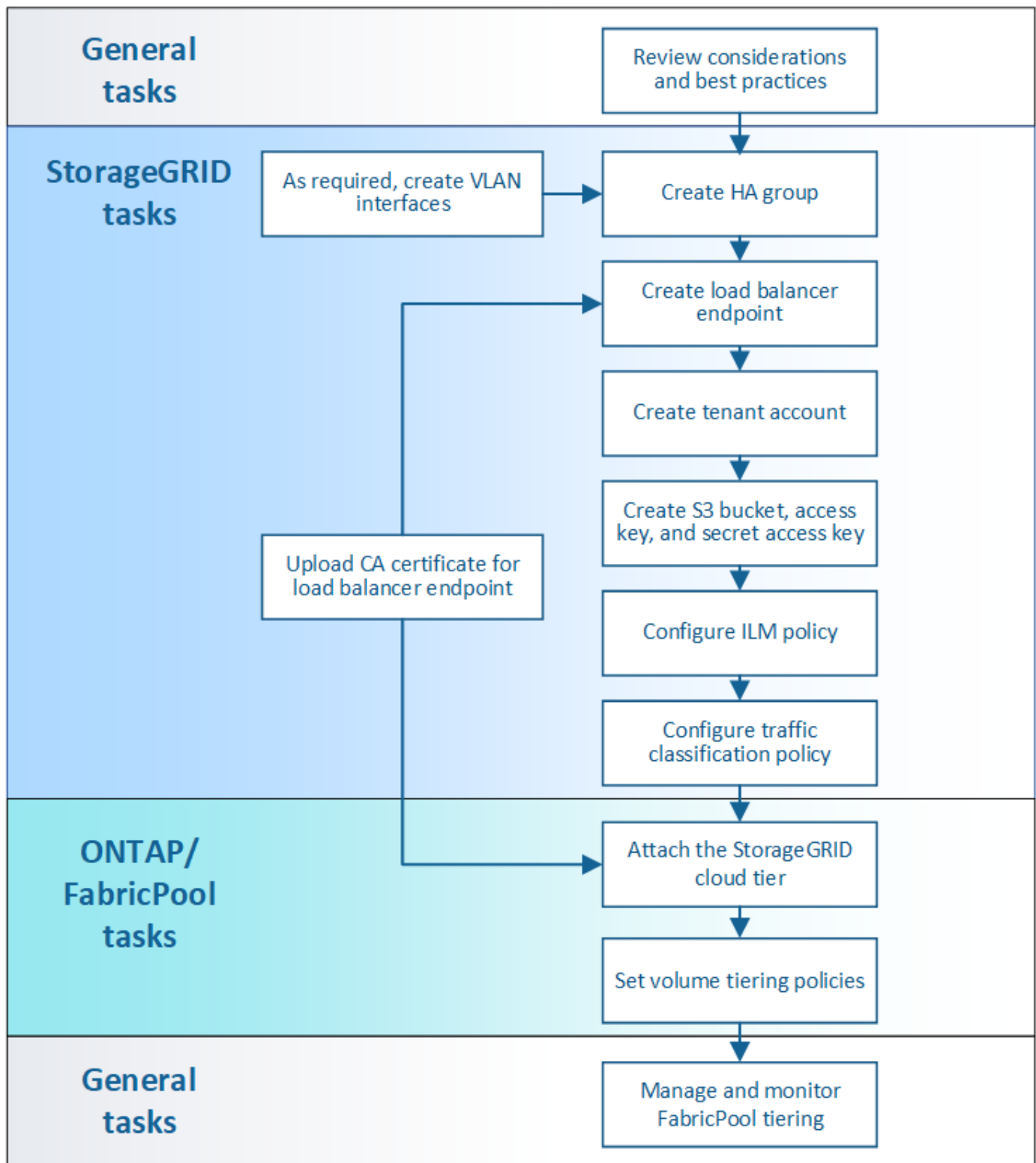
Si vous utilisez NetApp ONTAP, FabricPool vous pouvez effectuer le Tiering des données inactives ou inactives vers un système de stockage objet NetApp StorageGRID.

À propos de ces instructions

Suivez ces instructions pour :

- Découvrez comment configurer un système de stockage objet StorageGRID utilisé avec FabricPool.
- Découvrez comment obtenir les informations qu'il vous faut lorsque vous associez StorageGRID en tant que Tier cloud FabricPool à ONTAP.
- Découvrez les bonnes pratiques de configuration de la règle StorageGRID de gestion du cycle de vie des informations (ILM), une politique de classification du trafic StorageGRID et d'autres options StorageGRID pour une charge de travail FabricPool.

Flux de travail de configuration



Avant de commencer

- 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 grid et le

gestionnaire de locataires.

- Consultez les ressources supplémentaires suivantes, qui fournissent des informations détaillées sur l'utilisation et la configuration de FabricPool :
 - ["Tr-4598 : meilleures pratiques de FabricPool dans ONTAP 9.9.1"](#)
 - ["Documentation ONTAP 9"](#)

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 données sont stockées sur le support de stockage primaire ou dans le datastore d'objets, selon qu'elles soient utilisées fréquemment. Les agrégats compatibles FabricPool vous permettent de réduire les coûts de stockage sans nuire aux performances, à l'efficacité ou à la protection.

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 ?

StorageGRID est une architecture de stockage qui gère les données comme des objets, et non plus comme d'autres architectures de stockage, telles que le stockage de fichiers ou en blocs. Les objets sont conservés dans un seul conteneur (par exemple, un compartiment) et ne sont pas imbriqués dans un répertoire dans 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 procéder au Tiering des données ONTAP vers plusieurs fournisseurs de magasins d'objets, 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.

Est-il possible d'utiliser plusieurs clusters ONTAP avec StorageGRID ?

Ces instructions expliquent comment connecter StorageGRID à un seul cluster ONTAP. Vous pouvez cependant connecter le même système StorageGRID à plusieurs clusters ONTAP.

Vous devez utiliser un compartiment S3 différent pour chaque cluster afin de pouvoir effectuer le Tiering des données depuis plusieurs clusters ONTAP vers un seul système StorageGRID. Selon vos exigences, vous pouvez utiliser le même groupe haute disponibilité, le même point de terminaison d'équilibrage de charge et le même compte de locataire pour tous les clusters. Vous pouvez également configurer chacun de ces éléments pour chaque cluster.

Association de StorageGRID en tant que Tier cloud

Informations nécessaires pour rattacher StorageGRID à un niveau cloud

Avant de pouvoir associer StorageGRID en tant que Tier cloud pour FabricPool, vous devez effectuer certaines étapes de configuration dans StorageGRID et obtenir certaines valeurs.

Description de la tâche

Le tableau suivant répertorie les informations que vous devez fournir à ONTAP lorsque vous associez StorageGRID en tant que Tier cloud pour FabricPool. Les rubriques de cette section expliquent comment utiliser StorageGRID Grid Manager et le Gestionnaire de locataires pour obtenir les informations dont vous avez besoin.



Les noms de champ exacts répertoriés et le processus que vous utilisez pour entrer les valeurs requises dans ONTAP dépendent de l'utilisation de l'interface de ligne de commande ONTAP (Storage Aggregate Object-store config create) ou de ONTAP System Manager (**Storage Aggregates Disks Cloud Tier**).

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

- ["Tr-4598 : meilleures pratiques de FabricPool dans ONTAP 9.9.1"](#)
- ["Documentation ONTAP 9"](#)

Champ ONTAP	Description
Nom du magasin d'objets	Tout nom unique et descriptif. Par exemple : StorageGRID_Cloud_Tier.
Type de fournisseur	StorageGRID (ONTAP System Manager) ou SGWS (INTERFACE DE LIGNE DE COMMANDES ONTAP).
Port	Port utilisé par FabricPool lorsqu'il se connecte à StorageGRID. Vous déterminez le numéro de port à utiliser lorsque vous définissez le noeud final de l'équilibreur de charge StorageGRID. Créez un noeud final d'équilibrage de charge pour FabricPool

Champ ONTAP	Description
Nom du serveur	Nom de domaine complet (FQDN) pour le noeud final de l'équilibreur de charge StorageGRID. Par exemple : <code>s3.storagegrid.company.com</code>. Notez ce qui suit : • Le nom de domaine que vous spécifiez ici doit correspondre au nom de domaine sur le certificat d'autorité de certification que vous téléchargez pour le noeud final de l'équilibreur de charge StorageGRID. • L'enregistrement DNS de ce nom de domaine doit correspondre à chaque adresse IP que vous utiliserez pour vous connecter à StorageGRID. Configurez le serveur DNS pour les adresses IP StorageGRID
Nom du conteneur	Nom du compartiment StorageGRID que vous utiliserez avec ce cluster ONTAP. Par exemple : <code>fabricpool-bucket</code>. Il est possible de créer ce compartiment dans le Gestionnaire de locataires ou, en commençant par ONTAP 9.10 System Manager, il est possible de créer le compartiment à l'aide de l'assistant d'installation de FabricPool. Notez ce qui suit : • Le nom de compartiment ne peut pas être modifié une fois la configuration créée. • Le contrôle de version du compartiment ne peut pas être activé. • Vous devez utiliser un compartiment différent pour chaque cluster ONTAP afin de transférer les données vers StorageGRID. Créez un compartiment S3 et obtenez une clé d'accès
Clé d'accès et mot de passe secret	La clé d'accès et la clé secrète d'accès pour le compte de locataire StorageGRID. Ces valeurs sont générées dans le Gestionnaire de locataires. Créez un compartiment S3 et obtenez une clé d'accès
SSL	Doit être activé.

Champ ONTAP	Description
Certificat de magasin d'objets	Le certificat de l'autorité de certification que vous avez téléchargé lorsque vous avez créé le noeud final de l'équilibreur de charge StorageGRID. 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. Créez un noeud final d'équilibrage de charge pour FabricPool

Une fois que vous avez terminé

Une fois les informations StorageGRID requises obtenues, il est possible d'accéder à ONTAP pour ajouter StorageGRID comme Tier cloud, ajouter le niveau cloud en tant qu'agrégat et définir des règles de Tiering des volumes.

Bonnes pratiques pour l'équilibrage de la charge

Avant d'associer StorageGRID en tant que Tier cloud FabricPool, vous devez utiliser StorageGRID Grid Manager pour configurer au moins un noeud final d'équilibreur de charge.

Qu'est-ce que l'équilibrage de la charge ?

Lorsque les données sont placées dans un système FabricPool vers un système StorageGRID, StorageGRID utilise un équilibreur de charge afin de gérer le workload d'entrée et de récupération. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en distribuant la charge de travail FabricPool entre plusieurs nœuds de stockage.

Le service StorageGRID Load Balancer est installé sur tous les nœuds d'administration et sur tous les nœuds de passerelle. Il assure l'équilibrage de la charge de couche 7. Il effectue la résiliation du protocole TLS (transport Layer Security) des requêtes du client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage.

Le service Load Balancer de chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure.

Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de la charge recommandé, vous pouvez à la place intégrer un équilibreur de charge tiers. Pour plus d'informations, contactez votre ingénieur commercial NetApp ou consultez "[Tr-4626 : équilibreurs de charge mondiaux et tiers StorageGRID](#)".



Le service distinct Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète et n'est plus recommandé pour une utilisation avec FabricPool.

Bonnes pratiques pour l'équilibrage de la charge StorageGRID

Dans le cadre des meilleures pratiques générales, chaque site de votre système StorageGRID doit inclure au moins deux nœuds avec le service Load Balancer. Par exemple, un site peut inclure deux nœuds de

passerelle ou un nœud d'administration et un nœud de passerelle. S'assurer que l'infrastructure de mise en réseau, matérielle ou de virtualisation est adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services SG100 ou SG1000, des nœuds bare Metal ou des nœuds basés sur des machines virtuelles.

Vous devez configurer un nœud final d'équilibreur de charge StorageGRID pour définir le port que les nœuds de passerelle et les nœuds d'administration utiliseront pour les requêtes FabricPool entrantes et sortantes.

Bonnes pratiques pour le certificat de terminal de l'équilibreur de charge

Lors de la création d'un nœud final d'équilibrage de charge à utiliser avec FabricPool, vous devez utiliser HTTPS comme protocole. La communication avec StorageGRID sans chiffrement TLS est prise en charge mais non recommandée.

Vous pouvez ensuite télécharger un certificat signé par une autorité de certification publique ou privée ou générer un certificat auto-signé. Le certificat permet à ONTAP de s'authentifier auprès de StorageGRID.

Il est recommandé d'utiliser un certificat de serveur CA pour sécuriser la connexion. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption.

Lorsque vous demandez un certificat d'autorité de certification à utiliser avec le nœud final de l'équilibreur de charge, assurez-vous que le nom de domaine du certificat correspond au nom de serveur que vous entrez dans ONTAP pour ce nœud final de l'équilibreur de charge. Si possible, utilisez un caractère générique (*) pour autoriser les URL de type hôte virtuel. Par exemple :

```
*.s3.storagegrid.company.com
```

Lorsque vous ajoutez StorageGRID en tant que niveau cloud FabricPool, vous devez installer le même certificat sur le cluster ONTAP, ainsi que les certificats racine et toute autorité de certification subordonnée (CA).



StorageGRID utilise les certificats de serveur pour un certain nombre de raisons. Si vous vous connectez au service Load Balancer, vous pouvez éventuellement utiliser le certificat API S3 et Swift.

Pour en savoir plus sur le certificat de serveur pour un point final d'équilibrage de charge :

- [Configurer les terminaux de l'équilibreur de charge](#)
- [Consignes de renforcement des certificats de serveur](#)

Meilleures pratiques pour les groupes à haute disponibilité

Avant d'associer StorageGRID en tant que niveau cloud FabricPool, vous devez utiliser StorageGRID Grid Manager pour configurer un groupe haute disponibilité (HA).

Qu'est-ce qu'un groupe haute disponibilité ?

Pour s'assurer que le service Load Balancer est toujours disponible pour gérer les données FabricPool, vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans une seule entité, appelée groupe haute disponibilité. Si le nœud actif du groupe haute disponibilité tombe en panne, un autre nœud du groupe peut continuer à gérer le workload.

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 créer un groupe haute disponibilité, effectuez la procédure suivante :

1. Sélectionnez les interfaces réseau pour un ou plusieurs nœuds d'administration ou de passerelle. Vous pouvez sélectionner l'interface réseau Grid (eth0), l'interface réseau client (eth2) ou une interface VLAN.



Si vous envisagez d'utiliser une interface VLAN pour isoler le trafic FabricPool, un administrateur réseau doit d'abord configurer une interface de jonction et le VLAN correspondant. Chaque VLAN est identifié par un ID numérique ou une balise. Par exemple, votre réseau peut utiliser le VLAN 100 pour le trafic FabricPool.

2. Attribuez une ou plusieurs adresses IP virtuelles (VIP) au groupe. Les applications clients, telles que FabricPool, peuvent utiliser n'importe laquelle de ces adresses VIP pour se connecter à StorageGRID.
3. Spécifiez une interface à utiliser comme interface principale et déterminez l'ordre de priorité des interfaces de sauvegarde. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface principale échoue, les adresses VIP passent à 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. Ce 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.

Lorsque la 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.

Bonnes pratiques pour les groupes à haute disponibilité (HA)

Les bonnes pratiques de création d'un groupe StorageGRID HA pour FabricPool reposent sur le workload, comme suit :

- Si vous prévoyez d'utiliser FabricPool avec les données des principaux workloads, vous devez créer un groupe haute disponibilité incluant au moins deux nœuds d'équilibrage de la charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la règle de Tiering de volume FabricPool snapshot uniquement ou des tiers de performance locaux non principaux (par exemple, emplacements de reprise après incident ou destinations NetApp SnapMirror®), vous pouvez configurer un groupe haute disponibilité avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe haute disponibilité pour Active-Backup HA (un nœud est actif et un nœud est une sauvegarde). Cependant, vous préférez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour découvrir les avantages de ces autres configurations haute disponibilité, consultez [Options de configuration pour les groupes haute disponibilité](#).

Configurez le serveur DNS pour les adresses IP StorageGRID

Après avoir configuré des groupes de haute disponibilité et des nœuds finaux de l'équilibreur de charge, vous devez vous assurer que le système de noms de domaine (DNS) du système ONTAP inclut un enregistrement pour associer le nom de serveur StorageGRID (nom de domaine complet) à l'adresse IP que FabricPool utilisera 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, FabricPool se connecte aux adresses IP virtuelles de ce groupe haute disponibilité.
- Si vous n'utilisez pas de groupe haute disponibilité, FabricPool peut se connecter 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.

Créez un groupe haute disponibilité pour FabricPool

Lorsque vous configurez StorageGRID pour une utilisation avec FabricPool, vous pouvez éventuellement créer un ou plusieurs groupes haute disponibilité (HA). Un groupe haute disponibilité comprend une ou plusieurs interfaces réseau sur des nœuds d'administration ou de passerelle, ou les deux.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation accès racine.
- Si vous prévoyez d'utiliser un VLAN, vous avez créé l'interface VLAN. Voir [Configurez les interfaces VLAN](#).

Description de la tâche

Chaque groupe haute disponibilité utilise des adresses IP virtuelles (VIP) pour fournir un accès haute disponibilité aux services partagés sur les nœuds associés.

Pour plus d'informations sur cette tâche, reportez-vous à la section [Gérez les groupes haute disponibilité](#).

Étapes

1. Sélectionnez **CONFIGURATION réseau groupes haute disponibilité**.
2. Sélectionnez **Créer**.
3. Entrez un nom unique et éventuellement une description.
4. 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.

5. Déterminez l'interface principale et toutes les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser et déposez des lignes pour modifier les valeurs dans la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

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 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. Spécifiez le sous-réseau VIP dans la notation CIDR#8212;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.

7. 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.
8. Entrez une ou plusieurs adresses IP virtuelles pour le groupe haute disponibilité. Vous pouvez ajouter jusqu'à 10 adresses IP. Tous les VIP doivent être inclus dans le sous-réseau VIP.

Vous devez fournir au moins une adresse IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

9. Sélectionnez **Créer groupe HA**, puis **Terminer**.

Créez un noeud final d'équilibrage de charge pour FabricPool

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous devez configurer un noeud final de l'équilibreur de charge et télécharger le certificat de point final de l'équilibreur de charge, qui est utilisé pour sécuriser la connexion entre ONTAP et StorageGRID.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation d'accès racine.
- Vous disposez des fichiers suivants :
 - Certificat de serveur : fichier de certificat de serveur personnalisé.
 - Clé privée de certificat de serveur : fichier de clé privée de certificat de serveur personnalisé.
 - CA Bundle : fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (CA). 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.

Description de la tâche

Pour plus d'informations sur cette tâche, reportez-vous à la section [Configurer les terminaux de l'équilibreur de charge](#).

Étapes

1. Sélectionnez **CONFIGURATION réseau points d'extrémité de l'équilibreur de charge**.
2. Sélectionnez **Créer**.

×

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name ?

Port ?

Enter an unused port or accept the suggested port.

10443

Client type ?

Select the type of client application that will use this endpoint.

☒ S3
☐ Swift

Network protocol ?

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended)
☒ HTTP

Cancel

Continue

3. Saisissez les détails du point final.

Champ	Description
Nom	Un nom descriptif pour le noeud final
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est par défaut défini sur 10433, mais vous pouvez entrer tout port externe inutilisé. Si vous saisissez 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 réseau ne sont pas autorisés. Voir la Référence du port réseau. Vous devez fournir ce même numéro de port à ONTAP lorsque vous associez StorageGRID en tant que Tier cloud FabricPool.
Type de client	Sélectionnez S3 .

Champ	Description
Protocole réseau	Sélectionnez HTTPS. Remarque : l'utilisation de HTTP est prise en charge mais non recommandée.

4. Sélectionnez **Continuer**.

5. Spécifiez le mode de liaison.

Utilisez le paramètre **Global** (recommandé) ou limitez l'accessibilité de ce point final à l'un des paramètres suivants :

- Interfaces réseau spécifiques de nœuds spécifiques.
- Adresses IP virtuelles (VIP) haute disponibilité (HA) spécifiques. Utilisez cette sélection uniquement si vous avez besoin de niveaux d'isolation des charges de travail beaucoup plus élevés.

6. Sélectionnez **Continuer**.

7. Sélectionnez **Télécharger le certificat** (recommandé), puis naviguez jusqu'à votre certificat de serveur, votre clé privée de certificat et votre paquet CA facultatif.

8. Sélectionnez **Créer**.



Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Créez un compte de locataire pour FabricPool

Vous devez créer un compte de tenant dans le Grid Manager pour utilisation FabricPool.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

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.

Vous pouvez utiliser le même compte de locataire pour plusieurs clusters ONTAP. Vous pouvez également créer un compte de locataire dédié pour chaque cluster ONTAP, selon les besoins.



Ces instructions supposent que vous avez configuré l'authentification unique (SSO) pour Grid Manager. Si SSO n'est pas activé, utilisez [ces instructions permettent de créer un compte de locataire](#) à la place.

Étapes

1. Sélectionnez **LOCATAIRES**.

2. Sélectionnez **Créer**.

3. Entrez un nom d'affichage et une description.

4. Sélectionnez **S3**.
5. Laissez le champ **quota de stockage** vide.
6. Sélectionnez **Autoriser les services de plate-forme** pour activer l'utilisation des services de plate-forme.

Si les services de plateforme sont activés, un locataire peut utiliser des fonctionnalités, telles que la réplication CloudMirror, qui accèdent aux services externes.

7. Ne sélectionnez pas **utiliser son propre référentiel d'identité**.
8. Ne sélectionnez pas **Autoriser la sélection S3**.
9. Sélectionnez un groupe fédéré existant dans Grid Manager pour obtenir l'autorisation d'accès racine initiale du locataire.
10. Sélectionnez **Créer locataire**.

Créez un compartiment S3 et obtenez une clé d'accès

Avant d'utiliser StorageGRID avec un workload FabricPool, vous devez créer un compartiment S3 pour vos données FabricPool. Vous devez également obtenir une clé d'accès et une clé secrète pour le compte de locataire que vous utiliserez pour FabricPool.

Ce dont vous avez besoin

- Vous avez créé un compte de locataire pour l'utilisation de FabricPool.

Description de la tâche

Ces instructions expliquent comment utiliser le gestionnaire de locataires StorageGRID pour créer un compartiment et obtenir les clés d'accès. Vous pouvez également effectuer ces tâches à l'aide de l'API de gestion des locataires ou de l'API REST StorageGRID S3. Si vous utilisez ONTAP 9.10, vous pouvez également créer le compartiment à l'aide de l'assistant d'installation de FabricPool.

Pour en savoir plus :

- [Utilisez un compte de locataire](#)
- [Utilisation de S3](#)

Étapes

1. Connectez-vous au Gestionnaire de locataires.

Vous pouvez effectuer l'une des opérations suivantes :

- Dans la page comptes de tenant du Gestionnaire de grille, sélectionnez le lien **se connecter** pour le tenant et entrez vos informations d'identification.
- Saisissez l'URL du compte de tenant dans un navigateur Web et saisissez vos informations d'identification.

2. Créez un compartiment S3 pour les données FabricPool.

Vous devez créer un compartiment unique pour chaque cluster ONTAP que vous prévoyez d'utiliser.

- a. Sélectionnez **STOCKAGE (S3) seaux**.
- b. Sélectionnez **Créer un compartiment**.

- c. Entrez le nom du compartiment StorageGRID que vous utiliserez avec FabricPool. Par exemple : `fabricpool-bucket`.



Vous ne pouvez pas modifier le nom d'un compartiment après sa création.

Les noms de compartiment doivent être conformes aux règles suivantes :

- Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).
- Doit être conforme DNS.
- Doit contenir au moins 3 caractères et pas plus de 63 caractères.
- Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets.
- Ne doit pas ressembler à une adresse IP au format texte.
- Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur.

- d. Sélectionnez la région de ce compartiment.

Par défaut, tous les compartiments sont créés dans le `us-east-1` région.

Create bucket

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

fabricpool-bucket

Region ?

us-east-1

Cancel

Create bucket

- e. Sélectionnez **Créer un compartiment**.



Pour les compartiments FabricPool, le niveau de cohérence de compartiment recommandé est **Read-After-New-write**, qui est le paramètre par défaut d'un nouveau compartiment. Ne modifiez pas les compartiments FabricPool pour utiliser **disponible** ou tout autre niveau de cohérence.

3. Créez une clé d'accès et une clé d'accès secrète.

- a. Sélectionnez **STOCKAGE (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 créez une nouvelle clé d'accès et une clé secrète à l'avenir, n'oubliez pas de mettre à jour immédiatement les valeurs correspondantes dans ONTAP pour vous assurer que ONTAP peut stocker et récupérer les données dans StorageGRID sans interruption.

Utilisez la solution de gestion du cycle de vie des informations StorageGRID avec les données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez connaître les exigences de création des règles StorageGRID de gestion du cycle de vie des informations (ILM) et une règle ILM de gestion des données FabricPool. Vous devez veiller à ce que les règles ILM applicables aux données FabricPool ne soient pas perturbatrices.



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. Voir [Gestion des objets avec ILM](#) Pour obtenir des instructions détaillées relatives à l'ILM.

Ces recommandations vous permettent de vérifier que vos règles ILM et votre politique ILM conviennent pour les données FabricPool et les exigences de votre entreprise. Si vous utilisez déjà la solution ILM de StorageGRID, vous devrez peut-être mettre à jour votre politique ILM active pour respecter ces directives.

- 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.

- N'utilisez pas de règle ILM pour supprimer ou expirer les données de niveau cloud FabricPool. Définissez la période de conservation de chaque règle ILM sur « Forever » afin d'assurer la suppression des objets FabricPool par StorageGRID ILM.
- Ne créez pas de règles pour déplacer les données FabricPool de Tier cloud depuis le compartiment vers un autre emplacement. Vous ne pouvez pas utiliser les règles ILM pour archiver les données FabricPool sur bande à l'aide d'un nœud d'archivage ou utiliser un pool de stockage cloud pour les déplacer 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.

Exemple de règle ILM pour les données FabricPool

Utilisez cet exemple simple de règle comme point de départ pour vos propres règles et règles ILM.

Nous partons du principe que vous concevez les règles ILM et une règle ILM pour un système StorageGRID qui possède quatre nœuds de stockage dans un data Center unique à Denver, Colorado. Les données FabricPool dans cet exemple utilisent un compartiment nommé `fabricpool-bucket`.



Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte. Pour en savoir plus, voir [Gestion des objets avec ILM](#).

Étapes

1. Créez un pool de stockage nommé **DEN**. Sélectionnez le site Denver.
2. Créez un profil de code d'effacement nommé **2 plus 1**. Sélectionnez le schéma de code d'effacement 2+1 et le pool de stockage **DEN**.
3. Créez une règle ILM qui s'applique uniquement aux données dans `fabricpool-bucket`. Dans cet exemple de règle, des copies avec code d'effacement sont créées.

Définition de règle	Exemple de valeur
Nom de la règle	2 et 1 code d'effacement pour données FabricPool
Nom du compartiment	<code>fabricpool-bucket</code> Vous pouvez également filtrer le compte de tenant FabricPool.
Filtrage avancé	Taille de l'objet (Mo) supérieure à 0.2 Mo. Remarque : FabricPool écrit uniquement des objets de 4 Mo, mais vous devez ajouter un filtre de taille d'objet car cette règle utilise le codage d'effacement.

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Positionnement	À partir du jour 0 magasin pour toujours
Type	Code d'effacement
Emplacement	DEN (2 plus 1)
Comportement d'ingestion	Équilibré

4. Créez une règle ILM pour créer deux copies répliquées de tout objet ne correspondant pas à la première règle. Ne sélectionnez pas de filtre de base (compte de locataire ou nom de compartiment) ni de filtres avancés.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Nom du compartiment	<i>aucun</i>
Filtrage avancé	<i>aucun</i>
Heure de référence	Temps d'ingestion
Positionnement	À partir du jour 0 magasin pour toujours
Type	Copies Snapshot
Emplacement	DEN
Copies	2
Comportement d'ingestion	Équilibré

5. Création d'une règle ILM proposée et sélection des deux règles Comme la règle de réplication n'utilise aucun filtre, elle peut être la règle par défaut (dernière) de la règle.
6. Ingestion des objets de test dans la grille.
7. Simuler la règle avec les objets de test pour vérifier le comportement.
8. Activer la règle.

Lorsque cette règle est activée, StorageGRID place les données d'objet comme suit :

- Les données sont hiérarchisées à partir du système FabricPool In `fabricpool-bucket` le code d'effacement sera appliqué à l'aide du schéma de code d'effacement 2+1. Deux fragments de données et un fragment de parité seront placés sur trois nœuds de stockage différents.

- Tous les objets dans tous les autres compartiments sont répliqués. Deux copies sont créées et placées sur deux nœuds de stockage différents.
- Les copies répliquées et avec code d'effacement sont conservées dans StorageGRID jusqu'à leur suppression par le client S3. StorageGRID ILM ne supprimera jamais ces éléments.

Créer une règle de classification du trafic pour FabricPool

Vous pouvez éventuellement concevoir une règle de classification du trafic StorageGRID afin d'optimiser la qualité de service pour la charge de travail FabricPool.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur web pris en charge](#).
- Vous disposez de l'autorisation 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 mettre en Tier les données de la charge de travail principale FabricPool vers StorageGRID, assurez-vous que la charge de travail FabricPool dispose de la majorité 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, il n'est pas recommandé d'imposer des limites de qualité de service à un workload FabricPool ; vous ne devez limiter que les autres workloads.
- 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.

Pour en savoir plus : [Gérer les stratégies de classification du trafic](#)

Étapes

1. Sélectionnez **CONFIGURATION réseau classification du trafic**.
2. Entrez un nom et une description.
3. Dans la section règles de mise en correspondance, créez au moins une règle.
 - a. Sélectionnez **Créer**.
 - b. Sélectionnez **Endpoint**, 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 politique de trafic limite le trafic pour les autres noeuds finaux, sélectionnez **correspondance inverse**.

4. Vous pouvez éventuellement créer une ou plusieurs limites.



Même si aucune limite n'est définie pour une politique de classification du trafic, des métriques sont recueillies pour vous permettre de comprendre les tendances du trafic.

a. Sélectionnez **Créer**.

b. Sélectionnez le type de trafic que vous souhaitez limiter et la limite à appliquer.

Cet exemple de stratégie de classification de trafic FabricPool affiche les types de trafic réseau que vous pouvez limiter et les types de valeurs que vous pouvez sélectionner. Les limites d'une politique réelle dépendent de vos besoins spécifiques.

Policy

Name 

FabricPool

Description (optional)

Limit traffic other than FabricPool

Matching Rules

Traffic that matches any rule is included in the policy.

 Create

 Edit

 Remove

Type	Inverse Match	Match Value
☒ Endpoint		FabricPool (https 10443)

Displaying 1 matching rule.

Limits (Optional)

 Create

 Edit

 Remove

Type	Value	Units
☐ Concurrent Read Requests	50	Concurrent Requests
☐ Concurrent Read Requests	15	Concurrent Requests
☐ Read Request Rate	100	Requests/Second
☐ Write Request Rate	25	Requests/Second
☐ Per-Request Bandwidth In	2000000	Bytes/Second
☒ Per-Request Bandwidth Out	10000000	Bytes/Second

5. Après avoir créé la stratégie de classification du trafic, sélectionnez la stratégie, puis sélectionnez **métriques** pour déterminer si la stratégie limite le trafic comme prévu.

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
☒ FabricPool	Limit traffic other than FabricPool	587f53b2-7cf2-44b9-af5c-694ebbd4a2c5
Displaying 1 traffic classification policy.		

Autres meilleures pratiques pour StorageGRID et FabricPool

Lorsque vous configurez un système StorageGRID pour une utilisation avec FabricPool, vous devez éviter de définir des options globales susceptibles d'affecter la façon dont vos données sont enregistrées.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le paramètre global **cryptage d'objet stocké** si le chiffrement des données est requis pour d'autres clients StorageGRID (**CONFIGURATION système Options de grille**). Les données envoyées depuis FabricPool vers StorageGRID sont déjà chiffrées, ce qui signifie qu'il n'est pas nécessaire d'activer le paramètre StorageGRID. Les clés de chiffrement côté client sont la propriété de ONTAP.

Compression d'objet

Lors de la configuration de StorageGRID, n'activez pas le paramètre global **Compresser objets enregistrés** (**CONFIGURATION système Options de grille**). Les données envoyées depuis FabricPool vers StorageGRID sont déjà compressées. L'activation de **Compress objets stockés** ne réduit pas davantage la taille d'un objet.

Niveau de cohérence

Pour les compartiments FabricPool, le niveau de cohérence de compartiment recommandé est **Read-After-New-write**, qui est le paramètre par défaut d'un nouveau compartiment. Ne modifiez pas les compartiments FabricPool pour utiliser **disponible** ou tout autre niveau de cohérence.

Hiérarchisation FabricPool

Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour 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.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.