



Configurer et gérer

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-120/admin/index.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Sommaire

Configurer et gérer un système StorageGRID	1
Administrer StorageGRID	1
Administrer StorageGRID	1
Commencez à utiliser Grid Manager	1
Contrôlez l'accès à StorageGRID	28
\${post_edited_translations.segment}	76
Gérer la sécurité	116
Gérer les locataires	189
Configurer les connexions client	209
Gérer les réseaux et les connexions	254
Utilisez AutoSupport	275
Gérer les nœuds de stockage	290
Gérer les nœuds d'administration	304
Gérez les objets avec ILM	305
Gérez les objets avec ILM dans StorageGRID	305
\${post_edited_translations.segment}	306
Créez et attribuez des niveaux de stockage dans StorageGRID	328
\${post_edited_translations.segment}	331
\${post_edited_translations.segment}	339
Gérez les profils de code d'effacement dans StorageGRID	360
Configurer les régions S3 pour StorageGRID	363
Créer une règle ILM	365
Gérer les politiques ILM	382
Travaillez avec les règles ILM et les politiques ILM dans StorageGRID	399
Utilisez le verrouillage d'objet S3	403
\${post_edited_translations.segment}	412
Renforcement du système pour StorageGRID	433
Découvrez le renforcement du système pour StorageGRID	433
Recommandations de renforcement pour les mises à niveau logicielles StorageGRID	434
Recommandations de renforcement pour les réseaux StorageGRID	434
Recommandations de renforcement pour les nœuds StorageGRID	435
Recommandations de renforcement pour TLS et SSH dans StorageGRID	439
Recommandations de renforcement pour les journaux, les mots de passe et les messages d'audit dans StorageGRID	441
StorageGRID avec FabricPool	442
Flux de configuration pour l'utilisation de StorageGRID avec FabricPool	442
Informations nécessaires pour connecter StorageGRID en tant que niveau cloud FabricPool	444
Utilisez l'assistant d'installation FabricPool	445
Configurer StorageGRID manuellement	459
Configurez ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud FabricPool	470
Configurer les entrées du serveur DNS pour StorageGRID avec FabricPool	472
Meilleures pratiques StorageGRID pour FabricPool	472
Supprimez les données FabricPool de StorageGRID	477

Configurer et gérer un système StorageGRID

Administrer StorageGRID

Administrer StorageGRID

Utilisez ces instructions pour configurer et administrer un système StorageGRID.

À propos de ces instructions

Les principales tâches de configuration et d'administration StorageGRID vous permettent de :

- Utilisez le Gestionnaire de grille pour configurer les groupes et les utilisateurs
- Créez des comptes locataires pour permettre aux applications clientes S3 de stocker et de récupérer des objets
- Configurer et gérer les réseaux StorageGRID
- Configurez AutoSupport
- Gérer les paramètres du nœud

Avant de commencer

- Vous avez une compréhension générale du système StorageGRID.
- Vous possédez des connaissances assez détaillées des interpréteurs de commandes Linux, des réseaux et de la configuration matérielle des serveurs.

Commencez à utiliser Grid Manager

Configuration requise du navigateur Web pour StorageGRID

Vous devez utiliser un navigateur Web compatible.

Navigateur Web	Version minimale prise en charge
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Définissez la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimum	1280

Connectez-vous au gestionnaire de grille StorageGRID

Vous accédez à la page de connexion de Grid Manager en saisissant le domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur web compatible.

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non principaux. Vous pouvez vous connecter à Grid Manager sur n'importe quel nœud d'administration pour gérer le système StorageGRID. Cependant, certaines procédures de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

Se connecter au groupe HA

Si des nœuds d'administration sont inclus dans un groupe à haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe HA ou d'un domaine complet qui pointe vers cette 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 via le nœud d'administration principal, sauf si celui-ci n'est pas disponible. Voir ["Gérer les groupes à haute disponibilité"](#).

Utilisez l'authentification unique (SSO)

Les étapes de connexion sont légèrement différentes si ["L'authentification unique \(SSO\) a été configurée"](#).

Connectez-vous à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous utilisez un ["navigateur Web pris en charge"](#).
- Les cookies sont activés dans votre navigateur web.
- Vous appartenez à un groupe d'utilisateurs qui possède au moins une autorisation.
- Vous disposez de l'URL du Grid Manager :

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

Vous pouvez utiliser le domaine complet, l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe HA de nœuds d'administration.

Pour accéder au Grid Manager sur un port autre que le port par défaut pour HTTPS (443), incluez le numéro de port dans l'URL :

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



L'authentification unique (SSO) n'est pas disponible sur le port restreint de Grid Manager. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur web compatible.
2. Dans la barre d'adresse du navigateur, saisissez l'URL du Grid Manager.
3. Si vous recevez une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation de votre navigateur. Voir ["Gérer les certificats de sécurité"](#).

4. Connectez-vous au Grid Manager.

L'écran de connexion qui apparaît dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser l'authentification unique (SSO)

- a. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
- b. Sélectionnez **Se connecter**.

Utilisation de l'authentification unique (SSO)

- Si StorageGRID utilise l'authentification unique (SSO) et que c'est la première fois que vous accédez à l'URL sur ce navigateur :
 - i. Sélectionnez **Se connecter**. Vous pouvez laisser le 0 dans le champ Compte.
 - ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre organisation.

Par exemple, si StorageGRID utilise l'authentification unique (SSO) et que vous avez déjà accédé à Grid Manager ou à un compte locataire :

- A. Saisissez **0** (l'identifiant du compte pour le Grid Manager) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.
- B. Sélectionnez **Se connecter**.
- C. Connectez-vous avec vos identifiants SSO habituels sur la page de connexion SSO de votre organisation.

Une fois connecté, la page d'accueil du Grid Manager s'affiche et contient le tableau de bord. Pour savoir quelles informations sont fournies, consultez ["Afficher et gérer le tableau de bord"](#).

Connectez-vous à un autre nœud d'administration

Suivez ces étapes pour vous connecter à un autre nœud d'administration.

Ne pas utiliser l'authentification unique (SSO)

Étapes

1. Dans la barre d'adresse du navigateur, saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Indiquez le numéro de port si nécessaire.
2. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
3. Sélectionnez **Se connecter**.

Utilisation de l'authentification unique (SSO)

Si StorageGRID utilise l'authentification unique (SSO) et que vous vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

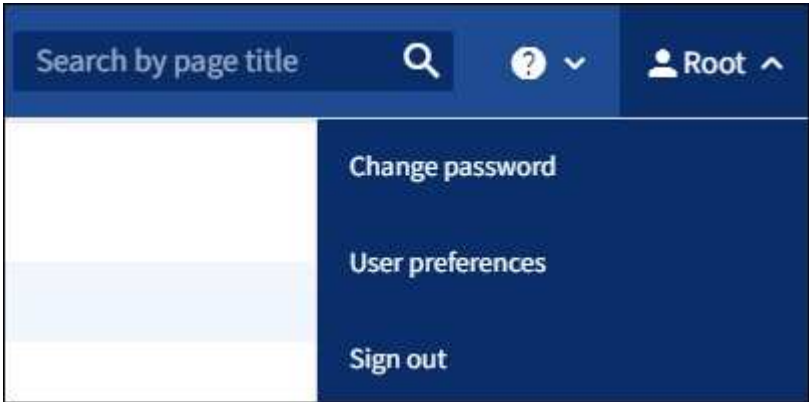
1. Saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, veuillez saisir à nouveau vos identifiants.

Déconnectez-vous du StorageGRID Grid Manager

Une fois votre session d'utilisation de Grid Manager terminée, vous devez vous déconnecter afin d'empêcher tout accès non autorisé au système StorageGRID. La fermeture de votre navigateur ne vous déconnectera pas nécessairement du système, selon les paramètres des cookies de votre navigateur.

Étapes

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



- 2. Sélectionnez **Se déconnecter**.

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 indiqué par défaut dans le menu déroulant Recent Accounts, et le champ Account ID affiche 0. Remarque : Si l'authentification unique (SSO) est activée et que vous êtes également connecté au Tenant Manager, vous devez également "déconnectez-vous du compte locataire" à "Déconnexion de SSO".

Modifiez votre mot de passe StorageGRID Grid Manager

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

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans Grid Manager. Vous devez alors modifier votre mot de passe dans la source d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête du Grid Manager, sélectionnez **your name** > **Change password**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

Votre mot de passe doit contenir au moins 8 et au plus 32 caractères. Les mots de passe sont sensibles à la casse.

4. Saisissez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Consultez les informations de licence StorageGRID

Vous pouvez consulter les informations de licence de votre système StorageGRID, telles que la capacité de stockage maximale de votre grille, à tout moment.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

En cas de problème de licence logicielle pour ce système StorageGRID, la carte « État de santé » du tableau de bord affiche une icône d'état de licence et un lien **Licence**. Le nombre indique le nombre de problèmes liés à la licence.



Étapes

1. Accédez à la page de licence en procédant de l'une des manières suivantes :
 - Sélectionnez **Maintenance** > **Système** > **Licence**.
 - Depuis la carte d'état de santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**.

Ce lien n'apparaît que s'il y a un problème avec la licence.

2. Consultez les détails en lecture seule de la licence actuelle :

- ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
- numéro de série de la licence
- Type de licence, soit **Perpetual** ou **Subscription**
- Capacité de stockage autorisée du grid
- Capacité de stockage prise en charge
- Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
- Date de fin de support

Cette date est extraite du fichier de licence actuel et peut être obsolète si vous avez prolongé ou renouvelé le contrat de service d'assistance après l'obtention du fichier de licence. Pour mettre à jour cette valeur, consultez "[Mettre à jour les informations de licence StorageGRID](#)". Vous pouvez également consulter la date de fin de contrat réelle à l'aide de Active IQ.

- Contenu du fichier texte de la licence

Mettre à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID chaque fois que les conditions de votre licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez une capacité de stockage supplémentaire pour votre grid.

Avant de commencer

- Vous disposez d'un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous disposez de la phrase secrète de provisionnement.

Étapes

1. Sélectionnez **Maintenance > Système > Licence**.
2. Dans la section Mise à jour de la licence, sélectionnez **Parcourir**.
3. Localisez et sélectionnez le nouveau fichier de licence (.txt).

Le nouveau fichier de licence est validé et affiché.

4. Saisissez la phrase secrète de provisionnement.
5. Sélectionnez **Enregistrer**.

Utilisez la ligne de commandes (API)

Utilisez l'API de gestion de grille StorageGRID

Vous pouvez effectuer des tâches de gestion système à l'aide de l'API REST de Grid Management plutôt qu'en utilisant l'interface utilisateur de Grid Manager. Par exemple, vous pourriez vouloir utiliser l'API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

L'API de gestion de grille fournit les ressources de premier niveau suivantes :

- `/grid` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées.
- `/org` : L'accès est limité aux utilisateurs appartenant à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, consultez ["Utilisez un compte locataire"](#).
- `/private` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

Émettre des requêtes API

L'API de gestion de la grille utilise la plateforme API open source Swagger. Swagger offre une interface utilisateur intuitive permettant aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

L'interface utilisateur Swagger fournit des informations et une documentation complètes pour chaque opération API.

Avant de commencer

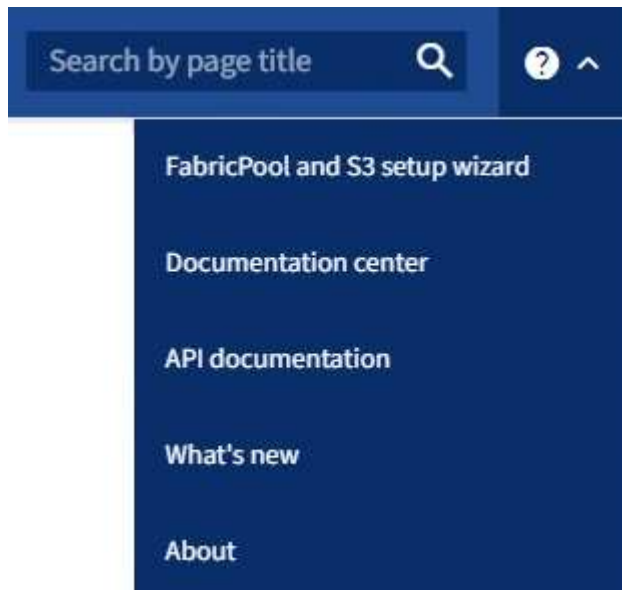
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).



Toute opération API effectuée via la page de documentation API est une opération en direct. Veuillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.



2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page de l'API de gestion StorageGRID.

Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

3. Sélectionnez l'opération souhaitée.

Lorsque vous développez une opération d'API, vous pouvez voir les actions HTTP disponibles, telles que GET, PUT, UPDATE et DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la requête, notamment l'URL du point de terminaison, la liste des paramètres obligatoires ou facultatifs, un exemple du corps de la requête (le cas échéant) et les réponses possibles.

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

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

Responses Response content 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>

5. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou

d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.

6. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.
7. Sélectionnez **Try it out**.
8. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
9. Sélectionnez **Exécuter**.
10. Examinez le code de réponse pour déterminer si la requête a réussi.

Opérations de l'API de gestion de la grille dans StorageGRID

L'API de gestion de grille organise les opérations disponibles dans les sections suivantes.



Cette liste ne comprend que les opérations disponibles dans l'API publique.

- **comptes** : Opérations permettant de gérer les comptes locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **historique des alertes** : opérations sur les alertes résolues.
- **récepteurs d'alertes** : Opérations sur les récepteurs de notifications d'alerte (courriel).
- **règles d'alerte** : Opérations sur les règles d'alerte.
- **silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : Opérations sur les alertes.
- **audit** : Opérations permettant de lister et de mettre à jour la configuration d'audit.
- **auth** : Opérations permettant d'authentifier la session utilisateur.

L'API Grid Management prend en charge le schéma d'authentification par jeton porteur. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la requête d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API suivantes (« `Authorization: Bearer token` »). Le jeton expire après 16 heures.



Si l'authentification unique est activée pour le système StorageGRID, vous devez suivre une procédure différente. Consultez la section « Authentification à l'API si l'authentification unique est activée ».

Consultez la section « Protection contre la falsification de requêtes intersites » pour obtenir des informations sur l'amélioration de la sécurité de l'authentification.

- **client-certificates** : Opérations permettant de configurer les certificats clients afin que StorageGRID puisse être accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **config** : Opérations relatives à la version du produit et aux versions de l'API de gestion de grille. Vous pouvez afficher la version de la publication du produit et les versions majeures de l'API de gestion de grille prises en charge par cette publication, et vous pouvez désactiver les versions obsolètes de l'API.
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **serveurs DNS** : Opérations permettant de lister et de modifier les serveurs DNS externes configurés.

- **drive-details** : Opérations sur les disques pour des modèles spécifiques d'appiances de stockage.
- **endpoint-domain-names** : Opérations permettant de lister et de modifier les noms de domaine des endpoints S3.
- **codage d'effacement** : opérations sur les profils de codage d'effacement.
- **expansion** : opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : Opérations sur l'expansion (niveau du nœud).
- **sites d'expansion** : Opérations sur l'expansion (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste du Grid Network.
- **grid-passwords** : Opérations pour la gestion des mots de passe de la grille.
- **Groupes** : Opérations permettant de gérer les groupes d'administrateurs de grille locaux et de récupérer les groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **identity-source** : Opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures** : Récupère les procédures de maintenance en cours.
- **licence** : Opérations permettant de récupérer et de mettre à jour la licence StorageGRID.
- **journaux** : Opérations de collecte et de téléchargement des fichiers journaux.v
- **Métriques** : Opérations sur les métriques StorageGRID, notamment les requêtes de métriques instantanées à un instant précis et les requêtes de métriques sur une plage de temps. L'API de gestion du réseau utilise l'outil de surveillance système Prometheus comme source de données principale. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site web de Prometheus.



Les indicateurs dont le nom contient *private* sont destinés à un usage interne uniquement. Ces indicateurs sont susceptibles d'être modifiés entre les versions de StorageGRID sans préavis.

- **node-details** : Opérations sur les détails du nœud.
- **node-health** : Opérations sur l'état de santé du nœud.
- **node-storage-state** : Opérations sur l'état du stockage des nœuds.
- **ntp-servers** : Opérations permettant de lister ou de mettre à jour les serveurs externes Network Time Protocol (NTP).
- **objets** : Opérations sur les objets et les métadonnées des objets.
- **récupération** : Opérations pour la procédure de récupération.
- **recovery-package** : Opérations de téléchargement du recovery package.
- **régions** : Opérations permettant de visualiser et de créer des régions.
- **s3-object-lock** : Opérations sur les paramètres globaux de verrouillage d'objet S3.
- **server-certificate** : Opérations permettant de consulter et de mettre à jour les certificats du serveur Grid Manager.
- **snmp** : Opérations sur la configuration SNMP actuelle.
- **storage-watermarks** : Filigranes des nœuds de stockage.
- **classes-de-traffic** : Opérations relatives aux politiques de classification du trafic.

- **untrusted-client-network** : Opérations sur la configuration du réseau client non fiable.
- **utilisateurs** : Opérations permettant de consulter et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API Grid Management dans StorageGRID

L'API de gestion de grille utilise le versionnage pour permettre des mises à niveau sans interruption de service.

Par exemple, cette URL de requête spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version majeure de l'API est mise à jour lorsque des modifications qui ne sont pas compatibles avec les versions précédentes sont apportées. La version mineure de l'API est mise à jour lorsque des modifications qui sont compatibles avec les versions précédentes sont apportées. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions antérieures	2,1	2,2
Non compatible avec les versions antérieures	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pendant au moins une version de StorageGRID.



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour "[API de gestion de grille](#)" plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API vers la nouvelle version.

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « `Deprecated: true` »
- Le corps de la réponse JSON inclut "`deprecated`": true
- Un avertissement de dépréciation est ajouté au fichier `nms.log`. Par exemple :

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Déterminez quelles versions d'API sont prises en charge dans la version actuelle

Utilisez la `GET /versions` requête API pour obtenir une liste des versions majeures de l'API prises en charge. Cette requête se trouve dans la section **config** de la documentation de l'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Spécifiez une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin (/api/v4) ou d'un en-tête (Api-Version: 4). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protégez-vous contre les attaques Cross-Site Request Forgery (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

Pour activer cette fonctionnalité, définissez le paramètre `csrfToken` sur `true` lors de l'authentification. La valeur par défaut est `false`.

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

Lorsque cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes susceptibles de modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- L'`X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie du jeton CSRF.
- Pour les points de terminaison qui acceptent un corps encodé sous forme de formulaire : un `csrfToken` paramètre de corps de requête encodé sous forme de formulaire.

Consultez la documentation API en ligne pour obtenir des exemples et des détails supplémentaires.



Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête "Content-Type: application/json" à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée

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

Si vous avez ["authentification unique \(SSO\) configurée et activée"](#) et que vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de la grille ou l'API de gestion des locataires.

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

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

Avant de commencer

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

À propos de cette tâche

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

- Le `storagegrid-ssoauth.py` script Python, qui se trouve dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

- Un exemple de workflow de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : A valid SubjectConfirmation was not found on this Response.



Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

Si vous rencontrez un problème d'encodage d'URL, vous pourriez voir l'erreur : Unsupported SAML version.

Étapes

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

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

- La méthode SSO. Saisissez ADFS ou adfs.
- Nom d'utilisateur SSO
- Le domaine sur lequel StorageGRID est installé
- L'adresse de StorageGRID
- L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

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

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

Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

3. Si vous souhaitez utiliser des requêtes curl, suivez la procédure suivante.
 - a. Déclarez les variables nécessaires à la connexion.


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



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

- b. Pour recevoir une URL d'authentification signée, envoyez une requête POST à `/api/v3/authorize-saml`, et supprimez l'encodage JSON supplémentaire de la réponse.

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

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

La réponse pour cet exemple inclut une URL signée et encodée en URL, mais elle n'inclut pas la couche d'encodage JSON supplémentaire.

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

- c. Enregistrez le SAMLRequest de la réponse pour l'utiliser dans les commandes suivantes.

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

- d. Obtenez une URL complète qui inclut l'ID de requête client depuis AD FS.

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

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

La réponse inclut l'identifiant de la requête du client :

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

e. Enregistrez l'identifiant de la requête client à partir de la réponse.

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

f. Envoyez vos identifiants à l'action du formulaire de la réponse précédente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS renvoie une redirection 302, avec des informations supplémentaires dans les en-têtes.



Si l'authentification multifactorielle (MFA) est activée pour votre système SSO, le formulaire envoyé 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...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs; HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Enregistrez le `MSISAuth` cookie issu de la réponse.

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

h. Envoyez une requête GET à l'emplacement spécifié avec les cookies issus de la requête 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 contiendront les informations de session AD FS pour une utilisation ultérieure lors de la déconnexion, et le corps de la réponse contient la SAMLResponse dans un champ de formulaire caché.

```
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
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj0lOVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Enregistrez le SAMLResponse du champ caché :

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

- j. À l'aide des données enregistrées `SAMLResponse`, effectuez une demande `StorageGRID/api/saml-response` pour générer un jeton d'authentification `StorageGRID`.

Pour `RelayState`, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la grille.

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

La réponse inclut le jeton d'authentification.

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

- a. Enregistrez le jeton d'authentification dans la réponse en tant que `MYTOKEN`.

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

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

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API `StorageGRID` depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis `StorageGRID`, ce qui requiert un jeton d'authentification `StorageGRID` valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `cookie "sso=true" à l'API SLO :

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

Une URL de déconnexion est renvoyée :

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envoyez une requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via l'API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Supprimez le jeton porteur StorageGRID.

La suppression du jeton d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

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

Une `204 No Content` réponse indique que l'utilisateur est maintenant déconnecté.

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

Utilisez l'API StorageGRID si l'authentification unique est activée (Entra ID)

Si vous avez "[authentification unique \(SSO\) configurée et activée](#)" et que vous utilisez Entra ID comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

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

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

Avant de commencer

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

À propos de cette tâche

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

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

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour créer votre propre intégration API avec Entra ID, consultez le script `storagegrid-ssoauth-azure.py`. Le script Python effectue deux requêtes directement à StorageGRID (la première pour obtenir la SAMLRequest, et la seconde pour obtenir le jeton d'autorisation), et appelle également le script Node.js pour interagir avec Entra ID afin d'effectuer les opérations SSO.

Les opérations d'authentification unique (SSO) peuvent être exécutées via une série de requêtes API, mais leur mise en œuvre n'est pas simple. Le module Puppeteer Node.js est utilisé pour extraire les données de l'interface SSO Entra ID.

Si vous rencontrez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

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

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

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

Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions SSO Entra ID.

3. Lorsque vous y êtes invité, saisissez les valeurs des arguments suivants (ou transmettez-les en tant que paramètres) :
 - L'adresse e-mail SSO utilisée pour vous connecter à Entra ID
 - L'adresse de StorageGRID
 - L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y serez invité, saisissez votre mot de passe et soyez prêt à fournir une autorisation MFA à Entra ID si cela vous est demandé.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Ce script suppose que l'authentification multifacteur (MFA) est effectuée via Microsoft Authenticator. Il se peut que vous deviez 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 le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

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

Si vous avez "[authentification unique \(SSO\) configurée et activée](#)" et que vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de la grille ou l'API de gestion des locataires.

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

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

Avant de commencer

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

À propos de cette tâche

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

- Le `storagegrid-ssoauth.py` script Python, qui se trouve dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de workflow de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response.`



Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

Si vous rencontrez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version.`

Étapes

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

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

- La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
- Nom d'utilisateur SSO
- Le domaine où StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou saisir une valeur quelconque.
- L'adresse de StorageGRID
- L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

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

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

Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

3. Si vous souhaitez utiliser des requêtes curl, suivez la procédure suivante.

a. Déclarez les variables nécessaires à la connexion.

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



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

b. Pour recevoir une URL d'authentification signée, envoyez une requête POST à /api/v3/authorize-saml, et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple illustre une requête POST pour obtenir une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool afin de supprimer l'encodage JSON.

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

La réponse pour cet exemple inclut une URL signée et encodée en URL, mais elle n'inclut pas la couche d'encodage JSON supplémentaire.

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

c. Enregistrez le SAMLRequest de la réponse pour l'utiliser dans les commandes suivantes.

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

d. Exportez la réponse et le cookie, puis affichez la réponse :

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

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

e. Exportez la valeur « pf.adapterId » et affichez la réponse :

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

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

f. Exportez la valeur « href » (supprimez la barre oblique finale /) et affichez la réponse :

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

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

g. Exportez la valeur « action » :

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

h. Envoyez les cookies avec les identifiants :

```
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 du champ caché :

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

j. À l'aide des données enregistrées SAMLResponse, effectuez une demande StorageGRID/api/saml-response pour générer un jeton d'authentification StorageGRID.

Pour RelayState, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la grille.

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

La réponse inclut le jeton d'authentification.

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

- a. Enregistrez le jeton d'authentification dans la réponse en tant que MYTOKEN.

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

Vous pouvez désormais utiliser MYTOKEN pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

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

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis StorageGRID, ce qui requiert un jeton d'authentification StorageGRID valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `cookie "sso=true" à l'API SLO :

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

Une URL de déconnexion est renvoyée :

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envoyez une requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via l'API uniquement.

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

4. Supprimez le jeton porteur StorageGRID.

La suppression du jeton d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

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

Une `204 No Content` réponse indique que l'utilisateur est maintenant déconnecté.

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

Désactivez les fonctionnalités de StorageGRID avec l'API

Vous pouvez utiliser l'API de gestion de la grille pour désactiver complètement certaines fonctionnalités dans le système StorageGRID. Lorsqu'une fonctionnalité est désactivée, personne ne peut se voir attribuer d'autorisations pour effectuer les tâches liées à cette fonctionnalité.

À propos de cette tâche

Le système de fonctionnalités désactivées vous permet d'empêcher l'accès à certaines fonctionnalités dans le système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur root ou les utilisateurs appartenant à des groupes d'administrateurs disposant de l'autorisation **Root access** d'utiliser cette fonctionnalité.

Pour comprendre en quoi cette fonctionnalité peut être utile, considérez le scénario suivant :

La société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes clients. Afin de protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne puissent jamais accéder à un compte client après son déploiement._

*Company A peut atteindre cet objectif en utilisant le système Deactivate Features dans l'API Grid Management. En désactivant complètement la fonctionnalité **Change tenant root password** dans le Grid Manager (à la fois dans l'interface utilisateur et dans l'API), Company A s'assure que les utilisateurs Admin — y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Root access** — ne peuvent pas modifier le mot de passe de l'utilisateur root de n'importe quel compte locataire._*

Étapes

1. Accédez à la documentation Swagger de l'API de gestion de grille. Voir ["Utilisez l'API de gestion de grille"](#).
2. Localisez le point de terminaison Deactivate Features.
3. Pour désactiver une fonctionnalité, telle que Change tenant root password, envoyez un corps à l'API comme ceci :

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

Lorsque la demande est terminée, la fonctionnalité Modifier le mot de passe root du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe root du locataire** n'apparaît plus dans l'interface utilisateur, et toute requête API qui tente de modifier le mot de passe root d'un locataire échouera avec "403 Forbidden."

Réactiver les fonctionnalités désactivées

Par défaut, vous pouvez utiliser l'API de gestion de la grille pour réactiver une fonctionnalité désactivée. Toutefois, si vous souhaitez empêcher que des fonctionnalités désactivées ne soient jamais réactivées, vous pouvez désactiver la fonctionnalité **activateFeatures** elle-même.



La fonctionnalité **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonctionnalité, sachez que vous perdrez définitivement la possibilité de réactiver toute autre fonctionnalité désactivée. Vous devez contacter le support technique pour rétablir toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation Swagger de l'API Grid Management.

2. Localisez le point de terminaison Deactivate Features.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps de requête à l'API comme ceci :

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

Une fois cette requête terminée, toutes les fonctionnalités, y compris la fonctionnalité **Changer le mot de passe racine du locataire**, sont réactivées. L'autorisation de gestion **Changer le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute requête API visant à modifier le mot de passe racine d'un locataire aboutira, à condition que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Changer le mot de passe racine du locataire**.



L'exemple précédent réactive *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent le rester, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité « Modifier le mot de passe racine du locataire » tout en continuant de désactiver l'autorisation de gestion storageAdmin, envoyez la requête PUT suivante :

```
{ "grid": {"storageAdmin": true} }
```

Contrôlez l'accès à StorageGRID

Contrôlez l'accès à StorageGRID

Vous contrôlez qui peut accéder à StorageGRID et quelles tâches les utilisateurs peuvent effectuer en créant ou en important des groupes et des utilisateurs, puis en attribuant des autorisations à chaque groupe. Vous pouvez également activer l'authentification unique (SSO), créer des certificats clients et modifier les mots de passe de la grille.

Contrôler l'accès au Grid Manager

Vous déterminez qui peut accéder à Grid Manager et à l'API de gestion de Grid en important des groupes et des utilisateurs à partir d'un service de fédération d'identités ou en configurant des groupes et des utilisateurs locaux.

L'utilisation de "[fédération d'identité](#)" permet de configurer "[groupes](#)" et "[utilisateurs](#)" plus rapidement, et elle permet aux utilisateurs de se connecter à StorageGRID avec leurs identifiants habituels. Vous pouvez configurer la fédération d'identité si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.



Contactez le support technique si vous souhaitez utiliser un autre service LDAP v3.

Vous déterminez les tâches que chaque utilisateur peut effectuer en attribuant différents "[autorisations](#)" à chaque groupe. Par exemple, vous pouvez vouloir que les utilisateurs d'un groupe puissent gérer les règles ILM et que ceux d'un autre groupe effectuent des tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

Vous pouvez éventuellement configurer un groupe en lecture seule. Les utilisateurs d'un groupe en lecture seule peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent effectuer aucune modification ni aucune opération dans Grid Manager ou Grid Management API.

Activer l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme Security

Assertion Markup Language 2.0 (SAML 2.0). Après que vous avez "[Configurer et activer l'authentification unique \(SSO\)](#)", tous les utilisateurs doivent être authentifiés par un fournisseur d'identité externe avant de pouvoir accéder au Grid Manager, au Tenant Manager, à l'API de gestion du Grid ou à l'API de gestion du Tenant. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifier la phrase secrète de provisionnement

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour télécharger le package de récupération StorageGRID. La phrase secrète est également requise pour télécharger les sauvegardes des informations de topologie du grid et les clés de chiffrement du système StorageGRID. Vous pouvez l'["modifier la phrase de passe"](#) utiliser selon vos besoins.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud, dont vous avez besoin pour vous connecter au nœud en tant qu'« admin » via SSH, ou en tant qu'utilisateur root sur une connexion console VM/physique. Au besoin, vous pouvez "[modifier le mot de passe de la console du nœud](#)" pour chaque nœud.

Modifier la phrase secrète de provisionnement StorageGRID

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous disposez des autorisations d'accès Maintenance ou Root.
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

La phrase de passe de configuration est requise pour de nombreuses procédures d'installation et de maintenance, et pour "[téléchargement du package de récupération](#)". La phrase de passe de configuration n'est pas indiquée dans le fichier `Passwords.txt`. Assurez-vous de documenter la phrase de passe de configuration et de la conserver en lieu sûr et sécurisé.

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Mots de passe de la grille**.
2. Sous **Modifier la phrase secrète de provisionnement**, sélectionnez **Effectuer une modification**.
3. Saisissez votre phrase secrète de provisionnement actuelle.
4. Saisissez la nouvelle phrase secrète. La phrase secrète doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases secrètes sont sensibles à la casse.



Conservez la phrase secrète de configuration dans un endroit sûr. Elle est requise pour l'installation, l'extension et la maintenance.

5. Saisissez à nouveau la nouvelle phrase secrète, puis sélectionnez **Enregistrer**.

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

 Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Sélectionnez **Recovery Package**.

7. Saisissez la nouvelle phrase secrète de provisionnement pour télécharger le nouveau package de récupération.



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

Modifier les mots de passe des consoles de nœud dans StorageGRID

Chaque nœud de votre grille possède un mot de passe de console, que vous utilisez pour vous connecter au nœud. Par défaut, chaque nœud possède un mot de passe unique. Vous pouvez modifier chaque mot de passe pour un nouveau mot de passe unique, ou vous pouvez modifier le mot de passe de chaque nœud afin d'utiliser un mot de passe global. Les mots de passe sont stockés dans le package de récupération.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès à la maintenance ou à la racine"](#).
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Vous utilisez un mot de passe de console de nœud pour vous connecter à un nœud en tant qu'« admin » via SSH, ou en tant qu'utilisateur root sur une connexion console VM/physique. Vous pouvez modifier les mots de passe de console de nœud à l'aide de l'une des options suivantes :

- Appliquer automatiquement des mots de passe aléatoires à chaque nœud
- Spécifiez et appliquez un mot de passe global à tous les nœuds
- Spécifiez et appliquez un mot de passe unique à un ou plusieurs nœuds

Les mots de passe sont stockés dans un fichier `Passwords.txt` mis à jour du package de récupération. Les mots de passe figurent dans la colonne « Mot de passe » de ce fichier.



Le ["mots de passe d'accès SSH"](#) des clés SSH utilisées pour la communication entre les nœuds est distinct des mots de passe de la console des nœuds. Cette procédure ne modifie pas les mots de passe d'accès SSH.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Mots de passe de la grille**.
2. Sous **Modifier les mots de passe de la console du nœud**, sélectionnez **Effectuer une modification**.

Télécharger le package de récupération actuel

Avant de modifier les mots de passe des consoles de nœuds, téléchargez le package de récupération actuel. Vous pouvez utiliser les mots de passe dans ce fichier si le processus de modification du mot de passe échoue pour un nœud.

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package de récupération**.
3. Copiez le fichier du package de récupération (.zip) vers deux emplacements sûrs, sécurisés et distincts.



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

4. Sélectionnez **Continue**.

Fournissez de nouveaux mots de passe

1. Sélectionnez la méthode de changement de mot de passe que vous souhaitez utiliser.
 - **Automatique** : StorageGRID attribue automatiquement un nouveau mot de passe de console aléatoire à tous les nœuds.
 - **Personnalisé** : Vous fournissez les mots de passe de la console.

Automatique

1. Sélectionnez **Continue**.

Personnalisé

1. Sélectionnez l'une des options suivantes :
 - **Mot de passe global de la console** : appliquez le même mot de passe de console à tous les nœuds.
 - **Mots de passe uniques pour la console** : appliquez un mot de passe différent sur un ou plusieurs nœuds.
2. Si vous avez sélectionné **Global console password**, saisissez le mot de passe que vous souhaitez utiliser pour tous les nœuds.
3. Si vous avez sélectionné **Mots de passe de console uniques**, saisissez un mot de passe unique pour un ou plusieurs nœuds.
4. Sélectionnez **Continue**.

Finalisez la modification du mot de passe

1. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à ce que StorageGRID commence à modifier les mots de passe de la console du nœud.



Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

StorageGRID génère un nouveau package de récupération contenant le nouveau mot de passe.

2. Lorsque le nouveau package de récupération est prêt, sélectionnez **Télécharger le nouveau package de récupération** et enregistrez le package de récupération.
3. Ouvrez le `.zip` fichier.
4. Confirmez que vous pouvez accéder au contenu, y compris au fichier `Passwords.txt` qui contient les nouveaux mots de passe de la console du nœud.
5. Copiez le nouveau fichier du package de récupération (`.zip` vers deux emplacements sûrs, sécurisés et distincts).



Ne remplacez pas l'ancien package de récupération.

Vous devez sécuriser le fichier de récupération, car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

6. Cochez la case pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
7. Sélectionnez **Continue**.

StorageGRID met à jour le mot de passe de chaque nœud.

En cas d'erreur lors du processus de mise à jour, la barre de progression indique le nombre de nœuds dont le mot de passe n'a pas pu être modifié. Le système réessaiera automatiquement le processus sur tout nœud dont le mot de passe n'a pas pu être modifié. Si le processus se termine avec certains nœuds dont le mot de passe n'a toujours pas été modifié, le bouton **Retry** apparaît.

8. Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :
 - a. Veuillez consulter les messages d'erreur répertoriés dans le tableau.
 - b. Résolvez les problèmes.
 - c. Sélectionnez **Réessayer**.



La nouvelle tentative ne modifie les mots de passe de la console des nœuds que sur les nœuds ayant échoué lors des précédentes tentatives de changement de mot de passe.

9. Lorsque la barre de progression indique qu'il ne reste plus de mises à jour, sélectionnez **Terminer**.
10. Une fois les mots de passe des consoles de nœuds modifiés pour tous les nœuds, supprimez le [premier package de récupération que vous avez téléchargé](#).

Modifier les mots de passe d'accès SSH pour les nœuds d'administration StorageGRID

La modification des mots de passe d'accès SSH des nœuds d'administration met également à jour les ensembles uniques de clés SSH internes de chaque nœud du grid. Le nœud d'administration principal utilise ces clés SSH pour accéder aux nœuds via une authentification sécurisée sans mot de passe.

Utilisez une clé SSH pour vous connecter à un nœud en `admin` ou à l'utilisateur `root` sur une VM ou une connexion console physique.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).

- Vous avez le "[Autorisation d'accès à la maintenance ou à la racine](#)".
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Les nouveaux mots de passe d'accès aux nœuds d'administration et les nouvelles clés internes de chaque nœud sont stockés dans le fichier `Passwords.txt` du package de récupération. Les clés sont indiquées dans la colonne « Mot de passe » de ce fichier.

Les clés SSH utilisées pour la communication entre les nœuds possèdent des mots de passe d'accès SSH distincts. Cette procédure ne les modifie pas.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Mots de passe de la grille**.
2. Sous **Changer les clés SSH**, sélectionnez **Apporter une modification**.

Télécharger le package de récupération actuel

Avant de modifier les clés d'accès SSH, téléchargez le package de récupération actuel. Vous pouvez utiliser les clés contenues dans ce fichier si le processus de modification échoue pour n'importe quel nœud.

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package de récupération**.
3. Copiez le fichier du package de récupération (`.zip` vers deux emplacements sûrs, sécurisés et distincts.



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

4. Sélectionnez **Continue**.
5. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les clés d'accès SSH.



Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les clés d'accès SSH

Lorsque le processus de modification des clés d'accès SSH démarre, un nouveau package de récupération contenant les nouvelles clés est généré. Ensuite, les clés sont mises à jour sur chaque nœud.

Étapes

1. Veuillez patienter pendant la génération du nouveau package de récupération, ce qui peut prendre quelques minutes.
2. Lorsque le bouton **Télécharger le nouveau package de récupération** est activé, sélectionnez **Télécharger le nouveau package de récupération** et enregistrez le nouveau fichier de package de récupération (`.zip` dans deux emplacements sûrs, sécurisés et distincts).
3. Une fois le téléchargement terminé :

- a. Ouvrez le `.zip` fichier.
- b. Vérifiez que vous pouvez accéder au contenu, y compris au fichier `Passwords.txt` qui contient les nouvelles clés d'accès SSH.
- c. Copiez le nouveau fichier du package de récupération (`.zip` vers deux emplacements sûrs, sécurisés et distincts).



Ne remplacez pas l'ancien package de récupération.

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

4. Attendez que les clés soient mises à jour sur chaque nœud, ce qui peut prendre quelques minutes.

Si les clés sont modifiées pour tous les nœuds, une bannière verte de succès apparaît.

En cas d'erreur lors de la mise à jour, un message d'avertissement indique le nombre de nœuds dont la clé n'a pas pu être modifiée. Le système réessaiera automatiquement la procédure sur tout nœud dont la clé n'a pas pu être modifiée. Si la procédure se termine avec certains nœuds n'ayant toujours pas de clé modifiée, le bouton **Retry** s'affiche.

Si la mise à jour de la clé a échoué pour un ou plusieurs nœuds :

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

La nouvelle tentative ne modifie que les clés d'accès SSH sur les nœuds qui ont échoué lors des précédentes tentatives de changement de clé.

5. Une fois les clés d'accès SSH modifiées pour tous les nœuds, supprimez le [premier package de récupération que vous avez téléchargé](#).
6. Vous pouvez également sélectionner **Maintenance > System > Recovery package** pour télécharger une copie supplémentaire du nouveau recovery package.

Utilisez la fédération d'identité dans StorageGRID

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

Configurer la fédération d'identités pour Grid Manager

Vous pouvez configurer la fédération d'identités dans Grid Manager si vous souhaitez que les groupes d'administrateurs et les utilisateurs soient gérés dans un autre système tel que Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous utilisez Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server comme

fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Directives pour la configuration d'un serveur OpenLDAP](#).
- Si vous prévoyez d'activer l'authentification unique (SSO), vous avez examiné le ["exigences et considérations pour l'authentification unique"](#).
- Si vous prévoyez d'utiliser le protocole TLS (Transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité utilise TLS 1.2 ou 1.3. Voir ["Chiffrements pris en charge pour les connexions TLS sortantes"](#).

À propos de cette tâche

Vous pouvez configurer une source d'identité pour Grid Manager si vous souhaitez importer des groupes depuis un autre système tel qu'Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administrateurs. Les utilisateurs appartenant aux groupes d'administrateurs peuvent se connecter à Grid Manager et effectuer des tâches, en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre source d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Tenant Manager et effectuer des tâches, en fonction des autorisations attribuées au groupe dans le Tenant Manager. Voir ["Créer un compte locataire"](#) et ["Utilisez un compte locataire"](#) pour plus de détails.

Saisissez la configuration

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Fédération d'identités**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section « Type de service LDAP », sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Sélectionnez **Autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **Autre**, complétez les champs de la section Attributs LDAP. Sinon, passez à l'étape suivante.
 - **Nom unique de l'utilisateur** : le nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` pour Active Directory et `uid` pour OpenLDAP. Si vous

configurez Oracle Directory Server, saisissez `uid`.

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

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

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



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

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

Pour Active Directory, vous pouvez également spécifier le nom d'ouverture de session de niveau inférieur ou le User Principal Name.

L'utilisateur spécifié doit avoir l'autorisation de lister les groupes et les utilisateurs et d'accéder aux attributs suivants :

- `sAMAccountName` ou `uid`
 - `objectGUID`, `entryUUID`, ou `nsuniqueid`
 - `cn`
 - `memberOf` ou `isMemberOf`
 - **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
 - **Entra ID** : `accountEnabled` et `userPrincipalName`
- **Mot de passe** : le mot de passe associé au nom d'utilisateur.



Si vous modifiez le mot de passe ultérieurement, vous devez le mettre à jour sur cette page.

- **DN de base du groupe** : le chemin complet du nom unique (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (`DC=storagegrid,DC=example,DC=com`)

peuvent être utilisés comme groupes fédérés.



Les valeurs du **nom unique du groupe** doivent être uniques au sein du **DN de base du groupe** auquel elles appartiennent.

- **DN de base utilisateur** : Le chemin complet du nom unique (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des utilisateurs.



Les valeurs du **nom unique de l'utilisateur** doivent être uniques au sein du **DN de base utilisateur** auquel elles appartiennent.

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

Il est recommandé de fournir le **format du nom d'utilisateur de liaison** car cela peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

Saisissez l'un de ces modèles :

- **UserPrincipalName modèle (AD et Entra ID)**: [USERNAME]@example.com
- **Modèle de nom d'ouverture de session de niveau inférieur (AD et Entra ID)** :
example\[USERNAME]
- **Modèle de nom unique** : CN=[USERNAME], CN=Users, DC=example, DC=com

Incluez [USERNAME] exactement comme écrit.

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

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



L'option « Ne pas utiliser TLS » n'est pas prise en charge si votre serveur Active Directory impose la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

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

- **Utiliser le certificat CA du système d'exploitation** : Utilisez le certificat CA Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **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 du certificat d'autorité de certification.

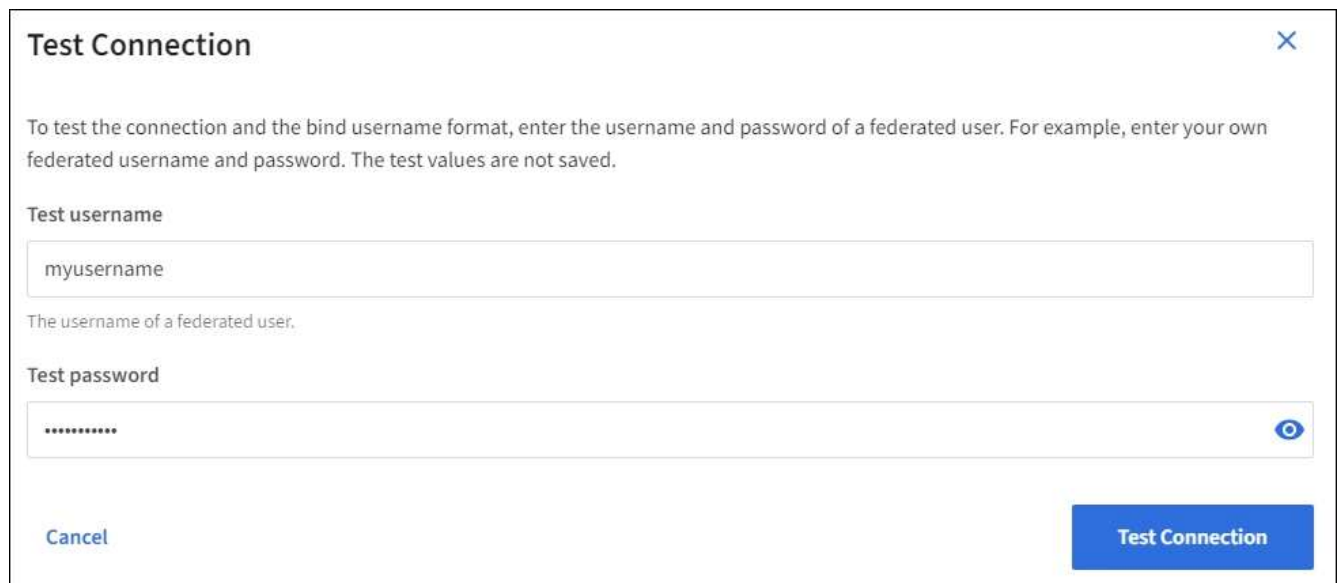
Testez la connexion et enregistrez la configuration

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

Étapes

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

Par exemple, saisissez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.



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

Forcer la synchronisation avec la source d'identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d'identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page de fédération d'identités.

2. Sélectionnez **Sync server** en haut de la page.

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



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

Désactivez la fédération d'identités

Vous pouvez désactiver temporairement ou définitivement la fédération d'identités pour les groupes et les utilisateurs. Lorsque la fédération d'identités est désactivée, il n'y a aucune communication entre StorageGRID et la source d'identités. Toutefois, les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités ultérieurement.

À propos de cette tâche

Avant de désactiver la fédération d'identités, vous devez prendre en compte les points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront plus se connecter après l'expiration de celle-ci.
- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et aucune alerte ne sera émise pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si le statut de l'authentification unique (SSO) est **Activé** ou **Mode bac à sable**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant que vous puissiez désactiver la fédération d'identités. Voir "[Désactivez l'authentification unique](#)".

Étapes

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

Directives pour la configuration d'un serveur OpenLDAP

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



Pour les sources d'identité autres qu'Active Directory ou Microsoft Entra ID, StorageGRID ne bloque pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou retirez l'utilisateur de tous les groupes.

Overlays Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la gestion des appartenances aux groupes inversées dans le "[Documentation OpenLDAP : Guide de l'administrateur version 2.4](#)".

Indexage

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

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

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

Consultez les informations relatives à la gestion des appartenances aux groupes inversés dans le ["Documentation OpenLDAP : Guide de l'administrateur version 2.4"](#).

Gérer les groupes d'administrateurs dans StorageGRID

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Si vous prévoyez d'importer un groupe fédéré, vous avez configuré la fédération d'identités et le groupe fédéré existe déjà dans la source d'identité configurée.

Créer un groupe d'administrateurs

Les groupes d'administrateurs vous permettent de déterminer quels utilisateurs peuvent accéder à quelles fonctionnalités et opérations dans le Grid Manager et l'API de gestion du Grid.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Groupes d'administrateurs**.
2. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs depuis la source d'identité.

Groupe local

Étapes

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d'affichage pour le groupe, que vous pourrez modifier ultérieurement si nécessaire. Par exemple, « Utilisateurs de maintenance » ou « ILM Administrators. »
3. Saisissez un nom unique pour le groupe, que vous ne pourrez pas modifier ultérieurement.
4. Sélectionnez **Continue**.

Groupe fédéré

Étapes

1. Sélectionnez **Groupe fédéré**.
2. Saisissez le nom du groupe que vous souhaitez importer, exactement comme il apparaît dans la source d'identité configurée.
 - Pour Active Directory et Microsoft Entra ID, utilisez le sAMAccountName.
 - Pour OpenLDAP, utilisez le CN (Common Name).
 - Pour un autre serveur LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continue**.

Gérer les autorisations de groupe

Étapes

1. Pour le **mode d'accès**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans Grid Manager et le Grid Management API, ou s'ils peuvent uniquement consulter les paramètres et les fonctionnalités.
 - **Lecture-écriture** (par défaut) : Les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs permissions de gestion.
 - **Lecture seule** : Les utilisateurs peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer d'opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent changer leur propre mot de passe.



Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en **Lecture seule**, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez-en un ou plusieurs "[autorisations du groupe d'administrateurs](#)".

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant au groupe ne pourront pas se connecter à StorageGRID.

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un groupe** puis **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

1. Facultativement, sélectionnez un ou plusieurs utilisateurs locaux pour ce groupe.

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

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

Afficher et modifier les groupes d'administrateurs

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

- Pour consulter les informations de base de tous les groupes, reportez-vous au tableau de la page Groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **Actions** ou la page de détails.

Tâche	Menu Actions	Page de détails
Afficher les détails du groupe	a. Cochez la case correspondant au groupe. b. Sélectionnez Actions > Afficher les détails du groupe .	Sélectionnez le nom du groupe dans le tableau.
Modifier le nom d’affichage (groupes locaux uniquement)	a. Cochez la case correspondant au groupe. b. Sélectionnez Actions > Modifier le nom du groupe . c. Saisissez le nouveau nom. d. Sélectionnez Save changes .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l’icône de modification  . c. Saisissez le nouveau nom. d. Sélectionnez Save changes .
Modifier le mode d’accès ou les autorisations	a. Cochez la case correspondant au groupe. b. Sélectionnez Actions > Afficher les détails du groupe . c. Vous pouvez éventuellement modifier le mode d’accès du groupe. d. Vous pouvez sélectionner ou effacer " autorisations du groupe d'administrateurs ". e. Sélectionnez Save changes .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Vous pouvez éventuellement modifier le mode d’accès du groupe. c. Vous pouvez sélectionner ou effacer " autorisations du groupe d'administrateurs ". d. Sélectionnez Save changes .

Dupliquer un groupe

Étapes

1. Cochez la case correspondant au groupe.
2. Sélectionnez **Actions > Dupliquer le groupe**.
3. Terminez l'assistant de duplication de groupe.

Supprimer un groupe

Vous pouvez supprimer un groupe d'administrateurs lorsque vous souhaitez le retirer du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe d'administrateurs retire tous les utilisateurs du groupe, mais ne supprime pas les utilisateurs.

Étapes

1. Sur la page Groupes, sélectionnez la case à cocher pour chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs dans StorageGRID

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

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter à Grid Manager ni à l'API de gestion de Grid.

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
- Consultez les pages des nœuds
- Afficher les alertes en cours et résolues
- Modifier leur propre mot de passe (utilisateurs locaux uniquement)
- Consultez certaines informations fournies sur les pages de configuration et de maintenance

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre **Mode d'accès** du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils peuvent uniquement consulter les paramètres et fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et que l'un d'eux est configuré en **Lecture seule**, l'utilisateur disposera d'un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administrateurs. Toute fonctionnalité non explicitement mentionnée requiert l'autorisation **Root access**.

Accès root

Cette autorisation donne accès à toutes les fonctionnalités d'administration du réseau.

Modifier le mot de passe root du locataire

Cette autorisation permet d'accéder à l'option **Modifier le mot de passe root** sur la page Locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur root local du locataire. Cette

autorisation est également utilisée pour la migration des clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe root**.



Pour accorder l'accès à la page Tenants, qui contient l'option **Change root password**, attribuez également l'autorisation **Tenant accounts**.

ILM

Cette autorisation donne accès aux options de menu **ILM** suivantes :

- Règles
- Politiques
- Étiquettes de stratégie
- Pools de stockage
- Classes de stockage
- Régions
- Recherche de métadonnées d'objet



Les utilisateurs doivent disposer de l'autorisation **Autre configuration de grille** pour gérer les niveaux de stockage.

Maintenance

Les utilisateurs doivent disposer de l'autorisation de maintenance pour utiliser ces options :

- **Configuration > Contrôle d'accès :**
 - Mots de passe de la grille
- **Configuration > Réseau :**
 - Noms de domaine des points de terminaison S3
- **Maintenance > Tâches :**
 - Mise hors service
 - Extension
 - Vérification de l'existence de l'objet
 - Récupération
- **Maintenance > Système :**
 - Package de récupération
 - Mise à jour logicielle
- **Assistance > Outils :**
 - Journaux

Les utilisateurs ne disposant pas de l'autorisation de maintenance peuvent consulter ces pages, mais pas les modifier :

- **Maintenance > Réseau :**

- Serveurs DNS
- Réseau Grid
- Serveurs NTP
- **Maintenance > Système :**
 - Licence
- **Configuration > Réseau :**
 - Noms de domaine des points de terminaison S3
- **Configuration > Sécurité :**
 - Certificats
- **Configuration > Surveillance :**
 - Serveur d'audit et de journalisation système

Gérer les alertes

Cette autorisation permet d'accéder aux options de gestion des alertes. Les utilisateurs doivent disposer de cette autorisation pour gérer les mises en sourdine, les notifications d'alerte et les règles d'alerte.

Requête de métriques

Cette autorisation donne accès à :

- **Support > Outils > Métriques** page
- Requêtes personnalisées sur les métriques Prometheus à l'aide de la section **Metrics** de l'API Grid Management
- Cartes du tableau de bord Grid Manager contenant des indicateurs

Recherche de métadonnées d'objet

Cette autorisation donne accès à la page **ILM > Recherche de métadonnées d'objet**.

Autre configuration de grille

Cette autorisation donne accès aux options de configuration de grille supplémentaires suivantes :

- **ILM:**
 - Classes de stockage
- **Configuration > Système :**
- **Assistance > Autre :**
 - Coût de liaison

Administrateur d'appliance de stockage

Cette autorisation permet :

- Accès au SANtricity System Manager de la série E sur les appliances de stockage via le Grid Manager.
- La possibilité d'effectuer des tâches de dépannage et de maintenance sur l'onglet Manage drives pour les appliances qui prennent en charge ces opérations.

Comptes de locataire

Cette autorisation permet de :

- Accédez à la page Locataires, où vous pouvez créer, modifier et supprimer des comptes locataires
- Consultez les politiques de classification du trafic existantes
- Consultez les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs dans StorageGRID

Vous pouvez consulter les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administrateurs locaux afin de déterminer les fonctionnalités de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Créer un utilisateur local

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

Vous pouvez uniquement créer des utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs et les groupes fédérés.

Le gestionnaire de grille inclut un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur root.



Si l'authentification unique (SSO) est activée, les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Utilisateurs administrateurs**.
2. Sélectionnez **Créer un utilisateur**.

Saisissez les identifiants de l'utilisateur

Étapes

1. Saisissez le nom complet de l'utilisateur, un nom d'utilisateur unique et un mot de passe.
2. Vous pouvez également sélectionner **Oui** si cet utilisateur ne doit pas avoir accès à Grid Manager ou à Grid Management API.
3. Sélectionnez **Continue**.

Attribuer aux groupes

Étapes

1. Vous pouvez, si vous le souhaitez, affecter l'utilisateur à un ou plusieurs groupes afin de déterminer les autorisations de l'utilisateur.

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

Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir ["Gérer les groupes d'administrateurs"](#) pour plus de détails.

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

Afficher et modifier les utilisateurs locaux

Vous pouvez consulter les informations des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour changer 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 pouvez uniquement modifier les utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs fédérés.

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

Les modifications sont appliquées lors de la prochaine déconnexion puis reconnexion de l'utilisateur au Grid Manager.



Les utilisateurs locaux peuvent modifier leur propre mot de passe en utilisant l'option **Changer le mot de passe** dans la bannière du Grid Manager.

Tâche	Menu Actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case pour 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 pour l'utilisateur. b. Sélectionnez Actions > Modifier le nom complet . c. Saisissez le nouveau nom. d. Sélectionnez Save changes .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône de modification  . c. Saisissez le nouveau nom. d. Sélectionnez Save changes .

Tâche	Menu Actions	Page de détails
Refuser ou autoriser l'accès à StorageGRID	a. Cochez la case pour 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 du Grid, ou sélectionnez Non pour autoriser l'utilisateur à se connecter. e. Sélectionnez Save changes.	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 du Grid, ou sélectionnez Non pour autoriser l'utilisateur à se connecter. d. Sélectionnez Save changes.
Changer le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case pour l'utilisateur. b. Sélectionnez Actions > Afficher les détails de l'utilisateur. c. Sélectionnez l'onglet Mot de passe. d. Saisissez un nouveau mot de passe. e. Sélectionnez Changer 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 Changer le mot de passe.
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case pour l'utilisateur. b. Sélectionnez Actions > Afficher les détails de l'utilisateur. c. Sélectionnez l'onglet Groupes. d. Vous pouvez également sélectionner le lien situé après le nom d'un groupe pour afficher les détails de ce groupe dans un nouvel onglet de votre navigateur. e. Sélectionnez Modifier les groupes pour sélectionner différents groupes. f. Sélectionnez Save changes.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Groupes. c. Vous pouvez également sélectionner le lien situé après le nom d'un groupe pour afficher les détails de ce groupe dans un nouvel onglet de votre navigateur. d. Sélectionnez Modifier les groupes pour sélectionner différents groupes. e. Sélectionnez Save changes.

Importer les utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Utilisateurs administrateurs.**
2. Sélectionnez **Importer les utilisateurs fédérés.**
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou de plusieurs utilisateurs fédérés.

Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

- Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
- Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Import federated users**.

Après la fermeture de la boîte de dialogue **Importer les utilisateurs fédérés**, les informations des utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur disposant des mêmes autorisations.

Étapes

- Cochez la case pour l'utilisateur.
- Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
- Terminez l'assistant de duplication d'utilisateur.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour le retirer définitivement du système.



Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

- Sur la page Utilisateurs, sélectionnez la case à cocher pour chaque utilisateur que vous souhaitez supprimer.
- Sélectionnez **Actions** > **Supprimer l'utilisateur**.
- Sélectionnez **Supprimer l'utilisateur**.

Utilisez l'authentification unique (SSO)

Découvrez l'authentification unique StorageGRID

Lorsque l'authentification unique (SSO) est activée, les utilisateurs peuvent accéder à Grid Manager, Tenant Manager, à l'API de gestion de Grid ou à l'API de gestion de locataires uniquement si leurs identifiants sont autorisés via le processus de connexion SSO mis en place par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Le système StorageGRID prend en charge l'authentification unique (SSO) utilisant la norme Security Assertion Markup Language 2.0 (SAML 2.0).

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

Connectez-vous lorsque l'authentification unique est activée

Lorsque l'authentification unique (SSO) est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d'identification.

Étapes

1. Saisissez le nom de domaine complet ou l'adresse IP de n'importe quel nœud d'administration StorageGRID dans un navigateur web.

La page de connexion StorageGRID s'affiche.

- Si c'est la première fois que vous accédez à l'URL sur ce navigateur, un identifiant de compte vous sera demandé.
- Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un identifiant de compte.



La page de connexion StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte locataire (c'est-à-dire un domaine complet ou une adresse IP suivis de `/?accountId=20-digit-account-id`). Vous êtes immédiatement redirigé vers la page de connexion SSO de votre organisation, où vous pouvez [Connectez-vous avec vos identifiants SSO](#).

2. Indiquez si vous souhaitez accéder au Grid Manager ou au Tenant Manager :
 - Pour accéder au Gestionnaire de grille, laissez le champ **ID du compte** vide, saisissez **0** comme ID du compte ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.
 - Pour accéder au Gestionnaire de locataires, saisissez l'identifiant du compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.
3. Sélectionnez **Sign in**

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

4. Connectez-vous avec vos identifiants SSO.

Si vos identifiants SSO sont corrects :

- a. Le fournisseur d'identité (IdP) fournit une réponse d'authentification à StorageGRID.
- b. StorageGRID valide la réponse d'authentification.
- c. Si la réponse est valide et que vous appartenez à un groupe fédéré disposant des autorisations d'accès à StorageGRID, vous êtes connecté au Grid Manager ou au Tenant Manager, selon le compte que vous avez sélectionné.



Si le compte de service est inaccessible, vous pouvez toujours vous connecter, à condition d'être un utilisateur existant appartenant à un groupe fédéré disposant des autorisations d'accès à StorageGRID.

5. Vous pouvez également accéder à d'autres Admin Nodes, ou au Grid Manager ou au Tenant Manager, si vous disposez des autorisations nécessaires.

Vous n'avez pas besoin de saisir à nouveau vos identifiants SSO.

Déconnectez-vous lorsque l'authentification unique est activée

Lorsque l'authentification unique (SSO) est activée pour StorageGRID, ce qui se passe lorsque vous vous déconnectez dépend de ce à quoi vous êtes connecté et de l'endroit d'où vous vous déconnectez.

Étapes

- 1. Repérez le lien **Se déconnecter** dans le coin supérieur droit de l'interface utilisateur.
- 2. Sélectionnez **Se déconnecter**.

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



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

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté(e) de...
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration Remarque : Si vous utilisez Entra ID pour l'authentification unique (SSO), il peut s'écouler quelques minutes avant que vous ne soyez déconnecté de tous les nœuds d'administration.
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	Uniquement le Grid Manager. Vous devez également vous déconnecter du Tenant Manager pour vous déconnecter de l'authentification unique (SSO).

Exigences et considérations relatives à l'authentification unique StorageGRID

Avant d'activer l'authentification unique (SSO) pour un système StorageGRID, examinez les exigences et les considérations.

Exigences du fournisseur d'identité

StorageGRID prend en charge les fournisseurs d'identité SSO (IdP) suivants :

- Service de fédération Active Directory (AD FS)
- Microsoft Entra ID

- PingFederate

Vous devez configurer la fédération d'identités pour votre système StorageGRID avant de pouvoir configurer un fournisseur d'identité SSO. Le type de service LDAP que vous utilisez pour la fédération d'identités détermine le type de SSO que vous pouvez implémenter.

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

Exigences AD FS

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

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



Windows Server 2016 doit utiliser la "[Mise à jour KB3201845](#)", ou une version supérieure.

Exigences supplémentaires

- Sécurité de la couche transport (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations relatives à Entra ID

Si vous utilisez Entra ID comme type d'authentification unique (SSO) et que les utilisateurs ont des noms principaux d'utilisateur qui n'utilisent pas sAMAccountName comme préfixe, des problèmes de connexion peuvent survenir si StorageGRID perd sa connexion avec le serveur LDAP. Pour permettre aux utilisateurs de se connecter, vous devez rétablir la connexion au serveur LDAP.

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au 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 parties de confiance (AD FS), des applications d'entreprise (Entra ID) ou des connexions de fournisseur de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les requêtes StorageGRID.

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



Il est déconseillé d'utiliser le certificat serveur par défaut d'un nœud d'administration dans une approbation de partie de confiance, une application d'entreprise ou une connexion SP. En cas de défaillance du nœud et de sa récupération, un nouveau certificat serveur par défaut est généré. Avant de pouvoir vous connecter au nœud récupéré, vous devez mettre à jour l'approbation de partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Exigences relatives aux ports

L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique. Voir ["Contrôler l'accès au niveau du pare-feu externe"](#).

Confirmez que les utilisateurs fédérés peuvent se connecter à StorageGRID

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au Tenant Manager pour tous les comptes locataires existants.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez déjà configuré la fédération d'identité.

Étapes

1. S'il existe des comptes locataires, vérifiez qu'aucun des locataires n'utilise sa propre source d'identité.



Lorsque vous activez l'authentification unique (SSO), la source d'identité configurée dans le Tenant Manager est remplacée par la source d'identité configurée dans le Grid Manager. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité du Grid Manager.

- a. Connectez-vous au Tenant Manager pour chaque compte locataire.
 - b. Sélectionnez **Gestion des accès > Fédération d'identités**.
 - c. Vérifiez que la case **Activer la fédération d'identités** n'est pas cochée.
 - d. Si c'est le cas, vérifiez que les groupes fédérés éventuellement utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
 - a. Dans Grid Manager, sélectionnez **Configuration > Contrôle d'accès > Groupes d'administrateurs**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et qu'il dispose de l'autorisation d'accès racine.
 - c. Déconnexion.

- d. Vérifiez que vous pouvez vous reconnecter à Grid Manager en tant qu'utilisateur du groupe fédéré.
3. S'il existe des comptes locataires, vérifiez qu'un utilisateur fédéré disposant de l'autorisation d'accès Root peut se connecter :
 - a. Dans le Gestionnaire de grille, sélectionnez **Locataires**.
 - b. Sélectionnez le compte du locataire, puis sélectionnez **Actions > Modifier**.
 - c. Dans l'onglet Saisir les détails, sélectionnez **Continuer**.
 - d. Si la case **Utiliser votre propre source d'identité** est cochée, décochez-la et sélectionnez **Enregistrer**.

La page du locataire s'affiche.

- e. Sélectionnez le compte locataire, sélectionnez **Se connecter**, puis connectez-vous au compte locataire en tant qu'utilisateur racine local.
- f. Dans le Gestionnaire de locataires, sélectionnez **Gestion des accès > Groupes**.
- g. Assurez-vous qu'au moins un groupe fédéré du Grid Manager s'est vu attribuer l'autorisation d'accès racine pour ce locataire.
- h. Déconnexion.
- i. Vérifiez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

- ["Exigences et considérations relatives à l'authentification unique"](#)
- ["Gérer les groupes d'administrateurs"](#)
- ["Utilisez un compte locataire"](#)

Configurer l'authentification unique (SSO) dans StorageGRID

Vous pouvez suivre l'assistant de configuration SSO et accéder au mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs de StorageGRID. Une fois l'authentification unique (SSO) activée, vous pouvez revenir au mode sandbox si nécessaire pour modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Vous avez configuré la fédération d'identités pour votre système StorageGRID.
- Pour le **type de service LDAP** de la fédération d'identités, vous avez sélectionné soit Active Directory, soit Entra ID, en fonction du fournisseur d'identités SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Service de fédération Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Entra ID	Entra ID

À propos de cette tâche

Lorsque l'authentification unique (SSO) est activée et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une requête d'authentification au fournisseur d'identité SSO. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la requête d'authentification a réussi. Pour les requêtes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Entra ID inclut un User Principal Name (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs, vous devrez effectuer les tâches suivantes :

1. Configurez les paramètres dans StorageGRID.
2. Utilisez le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Entra ID) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration.
3. Retournez à StorageGRID pour activer SSO.

Le mode bac à sable facilite les allers-retours de configuration et permet de tester tous vos paramètres avant d'activer l'authentification unique (SSO). Lorsque vous utilisez le mode bac à sable, les utilisateurs ne peuvent pas se connecter avec SSO.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**. La page d'authentification unique s'affiche.



Si le bouton Configurer les paramètres SSO est désactivé, vérifiez que vous avez bien configuré le fournisseur d'identité comme source d'identité fédérée. Consultez ["Exigences et considérations relatives à l'authentification unique"](#).

2. Sélectionnez **Configurer les paramètres SSO**. La page « Fournir les détails du fournisseur d'identité » s'affiche.

Fournissez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type d'authentification unique** dans la liste déroulante.
2. Si vous avez sélectionné Active Directory comme type SSO, saisissez le **nom du service de fédération** pour le fournisseur d'identité, exactement comme il apparaît dans Active Directory Federation Service (AD FS).



Pour trouver le nom du service de fédération, ouvrez le Gestionnaire de serveur Windows. Sélectionnez **Outils > Gestion d'AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération s'affiche dans le deuxième champ.

3. 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.
 - **Utiliser le certificat CA du système d'exploitation** : Utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
 - **Utiliser un certificat CA personnalisé** : Utilisez un certificat CA personnalisé pour sécuriser la connexion.

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

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



Si vous modifiez le certificat d'autorité de certification, "[Redémarrez le service mgmt-api sur les nœuds d'administration](#)" effectuez immédiatement cette opération et testez la réussite de l'authentification unique (SSO) dans Grid Manager.

4. Sélectionnez **Continuer**. La page « Fournir l'identifiant de la partie de confiance » s'affiche.

Fournissez l'identifiant de la partie de confiance

1. Remplissez les champs de la page « Fournir l'identifiant de la partie de confiance » en fonction du type d'authentification unique (SSO) que vous avez sélectionné.

Active Directory

- a. Spécifiez l'**identificateur de la partie de confiance** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'en ajouter d'autres à l'avenir, saisissez SG ou StorageGRID.
- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple, SG-[HOSTNAME]. Inclure cette chaîne génère un tableau affichant l'identifiant de la partie de confiance pour chaque nœud d'administration de la grille, en fonction du nom d'hôte du nœud.



Vous devez créer une relation de confiance avec une partie de confiance pour chaque nœud d'administration dans votre système StorageGRID. Le fait d'avoir une relation de confiance avec une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- b. Sélectionnez **Enregistrer et passer en mode bac à sable**.

Entra ID

- a. Dans la section Application d'entreprise, spécifiez le **nom de l'application d'entreprise** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque application d'entreprise dans Entra ID.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'en ajouter d'autres à l'avenir, saisissez SG ou StorageGRID.
- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple, SG-[HOSTNAME]. Inclure cette chaîne permet d'afficher un tableau présentant le nom de l'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. Le fait de disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- b. Suivez les étapes décrites dans "[Créez des applications d'entreprise dans Entra ID](#)" pour créer une application d'entreprise pour chaque Admin Node répertorié dans le tableau.
- c. À partir de Entra ID, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Collez ensuite cette URL dans le champ **URL des métadonnées de fédération** correspondant dans StorageGRID.
- d. Après avoir copié et collé une URL de métadonnées de fédération pour tous les Admin Nodes, sélectionnez **Enregistrer et entrer en mode sandbox**.

PingFederate

- a. Dans la section Fournisseur de services (SP), spécifiez l'**ID de connexion SP** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque connexion SP dans PingFederate.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'en ajouter d'autres à l'avenir, saisissez SG ou StorageGRID.

- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple, SG-[HOSTNAME]. Inclure cette chaîne génère un tableau affichant l'ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.



Vous devez créer une connexion SP pour chaque nœud d'administration dans votre système StorageGRID. Le fait d'avoir une connexion SP pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- b. Spécifiez l'URL des métadonnées de fédération pour chaque nœud d'administration dans le champ **Federation metadata URL**.

Utilisez le format suivant :

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- c. Sélectionnez **Enregistrer et passer en mode bac à sable**.

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

Après avoir enregistré la configuration et activé le mode sandbox, vous pouvez finaliser et tester la configuration pour le type de SSO que vous avez sélectionné.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, seuls les utilisateurs fédérés et les utilisateurs locaux peuvent se connecter.

Active Directory

Étapes

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

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

Pour obtenir des instructions, rendez-vous sur "[Créer des approbations de parties de confiance dans AD FS](#)".

Entra ID

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
 - a. Connectez-vous au nœud.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML de ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes décrites "[Créez des applications d'entreprise dans Entra ID](#)" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Entra ID correspondante.

PingFederate

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
 - a. Connectez-vous au nœud.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML de ce nœud.
3. Accédez à PingFederate.
4. "[Créez une ou plusieurs connexions de fournisseur de services \(SP\) pour StorageGRID](#)". Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué dans le tableau de la page Configurer l'authentification unique) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

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

Tester la configuration

Avant d'imposer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID,

vérifiez que l'authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d'administration.

Active Directory

Étapes

1. Sur la page Configurer SSO, repérez le lien à l'étape Tester la configuration de l'assistant.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Federation service name**.

2. Sélectionnez le lien, ou copiez et collez l'URL dans un navigateur, pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à StorageGRID, sélectionnez **Se connecter à l'un des sites suivants**, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal, puis sélectionnez **Se connecter**.
4. Saisissez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
 - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Entra ID

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
 - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Sur la page Configurer l'authentification unique (SSO), sélectionnez le premier lien du message relatif au mode Sandbox.

Sélectionnez et testez un lien à la fois.
2. Saisissez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
 - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO de chaque nœud d'administration de votre grille.

Si vous voyez un message « Page expirée », sélectionnez le bouton **Retour** de votre navigateur et soumettez à nouveau vos identifiants.

Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à chaque nœud d'administration, vous pouvez activer l'authentification unique (SSO) pour l'ensemble de votre système StorageGRID.



Lorsque l'authentification unique (SSO) est activée, tous les utilisateurs doivent utiliser SSO pour accéder au Grid Manager, au Tenant Manager, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. À l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Examinez le message d'avertissement et sélectionnez **Activer SSO**.

L'authentification unique est désormais activée. La page d'authentification unique s'affiche et contient désormais les informations relatives à l'authentification unique que vous venez de configurer.

3. Pour modifier la configuration, sélectionnez **Modifier**.
4. Pour désactiver l'authentification unique, sélectionnez **Désactiver SSO**.



Si vous utilisez le portail Azure et que vous accédez à StorageGRID depuis le même ordinateur que celui utilisé pour accéder à Entra ID, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (un utilisateur appartenant à un groupe fédéré qui a été importé dans StorageGRID), ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des approbations de parties de confiance dans AD FS pour StorageGRID

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

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous connaissez le domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau des détails des nœuds d'administration sur la page Configurer SSO de StorageGRID.



Vous devez créer une relation de confiance avec une partie de confiance pour chaque nœud d'administration dans votre système StorageGRID. Le fait d'avoir une relation de confiance avec une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'approbations de parties de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable Gestion AD FS et vous appartenez au groupe Administrators.
- Si vous créez manuellement la relation de confiance avec la partie de confiance, vous disposez du certificat personnalisé qui a été téléchargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir de l'invite de commandes.

À propos de cette tâche

Ces instructions concernent Windows Server 2016 AD FS. Si vous utilisez une autre version d'AD FS, vous constaterez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une relation d'approbation de partie de confiance à l'aide de Windows PowerShell

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

Étapes

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

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

- Pour *Admin_Node_Identifier*, saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement comme il apparaît sur la page d'authentification unique. Par exemple, SG-DC1-ADM1.
- Pour *Admin_Node_FQDN*, saisissez le domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > Gestion d'AD FS**.

L'outil de gestion AD FS apparaît.

4. Sélectionnez **AD FS > Approbations de parties de confiance**.

La liste des relations d'approbation de parties approuvées apparaît.

5. Ajoutez une stratégie de contrôle d'accès à l'approbation de partie de confiance nouvellement créée :
 - a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.
 - b. Cliquez avec le bouton droit sur l'approbation, puis sélectionnez **Modifier la stratégie de contrôle d'accès**.

- c. Sélectionnez une politique de contrôle d'accès.
- d. Sélectionnez **Appliquer**, puis **OK**
- 6. Ajoutez une politique d'émission de revendications à la nouvelle relation de confiance de partie utilisatrice :
 - a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.
 - b. Cliquez avec le bouton droit sur la fiducie, puis sélectionnez **Modifier la politique d'émission des revendications**.
 - c. Sélectionnez **Ajouter une règle**.
 - d. Sur la page Sélectionner le modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
 - e. Sur la page Configurer la règle, saisissez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

- f. Pour le magasin d'attributs, sélectionnez **Active Directory**.
- g. Dans la colonne Attribut LDAP du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
- h. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.
- i. Sélectionnez **Terminer**, puis sélectionnez **OK**.
- 7. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit sur l'entité de confiance pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de la fédération est correcte ou saisissez les valeurs manuellement.

- 8. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
- 9. Une fois que vous avez terminé, retournez sur StorageGRID "[tester toutes les relations d'approbation des parties dépendantes](#)" pour confirmer qu'ils sont correctement configurés.

Créez une relation de confiance de partie utilisatrice en important les métadonnées de fédération

Vous pouvez importer les valeurs de chaque approbation de partie de confiance en accédant aux métadonnées SAML de chaque Admin Node.

Étapes

- 1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
- 2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
- 3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
- 4. Sélectionnez **Importer les données relatives à la partie de confiance publiées en ligne ou sur un réseau local**.
- 5. Dans **Adresse des métadonnées de la fédération (nom de l'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour cet Admin Node :

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

Pour *Admin_Node_FQDN*, saisissez le domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)

6. Terminez l'assistant de création de la fiducie de partie de confiance, enregistrez la fiducie de partie de confiance et fermez l'assistant.



Lors de la saisie du nom d'affichage, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le Grid Manager. Par exemple, SG-DC1-ADM1.

7. Ajouter une règle de revendication :
 - a. Cliquez avec le bouton droit sur la fiducie, puis sélectionnez **Modifier la politique d'émission des revendications**.
 - b. Sélectionnez **Ajouter une règle** :
 - c. Sur la page Sélectionner le modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
 - d. Sur la page Configurer la règle, saisissez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

- e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - f. Dans la colonne Attribut LDAP du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
 - g. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.
 - h. Sélectionnez **Terminer**, puis sélectionnez **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit sur l'entité de confiance pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de la fédération est correcte ou saisissez les valeurs manuellement.

9. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
10. Une fois que vous avez terminé, retournez sur StorageGRID et "[tester toutes les relations d'approbation des parties dépendantes](#)" pour confirmer qu'ils sont correctement configurés.

Créer manuellement une relation de confiance avec une partie utilisatrice

Si vous choisissez de ne pas importer les données pour les approbations de la partie dépendante, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
4. Sélectionnez **Saisir manuellement les données relatives à la partie de confiance**, puis sélectionnez **Suivant**.
5. Terminez l'assistant de création de fiducie de partie de confiance :

- a. Saisissez un nom d'affichage pour ce nœud d'administration.

Par souci de cohérence, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le Grid Manager. Par exemple, SG-DC1-ADM1.

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

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

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

- e. Sur la page Configurer les identifiants, spécifiez l'identifiant de la partie de confiance pour le même nœud d'administration :

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement comme il apparaît sur la page d'authentification unique. Par exemple, SG-DC1-ADM1.

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

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



Si la boîte de dialogue n'apparaît pas, cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission des revendications**.

6. Pour démarrer l'assistant de règle de revendication, sélectionnez **Ajouter une règle** :
 - a. Sur la page Sélectionner le modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
 - b. Sur la page Configurer la règle, saisissez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.
 - c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - d. Dans la colonne Attribut LDAP du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-**

Principal-Name.

- e. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.
 - f. Sélectionnez **Terminer**, puis sélectionnez **OK**.
7. Cliquez avec le bouton droit sur l'entité de confiance pour ouvrir ses propriétés.
 8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :

- a. Sélectionnez **Ajouter SAML**.
- b. Sélectionnez **Type de point de terminaison > Déconnexion SAML**.
- c. Sélectionnez **Liaison > Redirection**.

- d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce Admin Node :

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

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

- a. Sélectionnez **OK**.
9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour cette approbation de partie de confiance :
- a. Ajouter le certificat personnalisé :
- Si vous avez téléchargé le certificat de gestion personnalisé sur StorageGRID, sélectionnez ce certificat.
 - Si vous ne possédez pas le certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.



L'utilisation du certificat par défaut du nœud d'administration (`server.crt`) n'est pas recommandée. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lors de la restauration du nœud, et vous devrez mettre à jour la relation de confiance de la partie dépendante.

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

Les propriétés de la partie utilisatrice sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
11. Une fois que vous avez terminé, retournez sur StorageGRID et "[tester toutes les relations d'approbation des parties dépendantes](#)" pour confirmer qu'ils sont correctement configurés.

Créez des applications d'entreprise dans Entra ID pour StorageGRID

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

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Entra ID** comme type de SSO.
- Vous avez **"mode bac à sable activé"** dans Grid Manager.
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs depuis le tableau des détails du nœud d'administration sur la page Configurer SSO.



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

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Entra ID.
- Vous possédez un compte Entra ID avec un abonnement actif.
- Vous possédez l'un des rôles suivants dans le compte Entra ID : Global Administrator, Cloud Application Administrator, Application Administrator ou owner of the service principal.

Accéder à Entra ID

Étapes

1. Connectez-vous à l' **"Portail Azure"**.
2. Accédez à **"Entra ID"**.
3. Sélectionnez **"Applications d'entreprise"**.

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

Pour enregistrer la configuration SSO d'Entra ID dans StorageGRID, vous devez utiliser Entra ID pour créer une application d'entreprise pour chaque Admin Node. Vous copierez les URL des métadonnées de fédération depuis Entra ID et les collerez dans les champs correspondants **Federation metadata URL** sur la page Configurer SSO.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
 - a. Dans le volet Applications d'entreprise d'Entra ID, sélectionnez **Nouvelle application**.
 - b. Sélectionnez **Créer votre propre application**.
 - c. Pour le nom, saisissez le **nom de l'application d'entreprise** que vous avez copié du tableau des détails du nœud d'administration sur la page Configurer SSO.
 - d. Laissez l'option **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionnée.
 - e. Sélectionnez **Create**.
 - f. Sélectionnez le lien **Get started** dans la **2. Set up single sign on** box, ou sélectionnez le lien **Single sign-on** dans la marge de gauche.
 - g. Sélectionnez la case **SAML**.
 - h. Copiez l'**App Federation Metadata Url**, que vous trouverez sous **Step 3 SAML Signing Certificate**.
 - i. Accédez à la page Configurer SSO, puis collez l'URL dans le champ **Federation metadata URL** qui

correspond au **Enterprise application name** que vous avez utilisé.

2. Après avoir collé une URL de métadonnées de fédération pour chaque Admin Node et effectué toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page Configurer SSO.

Téléchargez les métadonnées SAML pour chaque nœud d'administration

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

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.
 - a. Connectez-vous à StorageGRID depuis le nœud d'administration.
 - b. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - c. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
 - d. Enregistrez le fichier, que vous téléchargerez ensuite dans Entra ID.

Téléversez les métadonnées SAML dans chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID, effectuez les étapes suivantes dans Entra ID :

Étapes

1. Retournez au portail Azure.
2. Répétez ces étapes pour chaque application d'entreprise :



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

- a. Accédez à la page Propriétés de l'application d'entreprise.
 - b. Définissez **Assignment required** sur **Non** (sauf si vous souhaitez configurer les affectations séparément).
 - c. Accédez à la page d'authentification unique.
 - d. Finalisez la configuration SAML.
 - e. Sélectionnez le bouton **Téléverser un 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 êtes renvoyé à la page Configurer l'authentification unique avec SAML.
3. "[Tester chaque application](#)".

Créez des connexions de fournisseur de services dans PingFederate pour StorageGRID

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 allez importer les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type de SSO.
- Vous avez "[mode bac à sable activé](#)" dans Grid Manager.
- Vous disposez de l'**ID de connexion SP** pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau des détails des nœuds d'administration sur la page Configurer le SSO.
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans le serveur PingFederate.
- Vous disposez du "[Guide de référence de l'administrateur](#)" pour le serveur PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous disposez du "[Autorisation d'administrateur](#)" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer le serveur PingFederate 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. Consultez la documentation du serveur PingFederate pour obtenir des instructions détaillées concernant votre version.

Effectuez les prérequis 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 issues de ces prérequis lors de la configuration des connexions SP.

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 lors de "[configuration de la fédération d'identités](#)" dans StorageGRID.

- **Type** : Annuaire (LDAP)
- **Type LDAP** : Active Directory
- **Nom de l'attribut binaire** : Saisissez **objectGUID** dans l'onglet Attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'identifiants de mot de passe

Si ce n'est pas déjà fait, créez un validateur d'identifiants de mot de passe.

- **Type** : Validateur d'identifiant nom d'utilisateur/mot de passe LDAP
- **Magasin de données** : Sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : Saisissez les informations provenant de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=\${username}
- **Portée** : Sous-arbre

Créer une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP.

Étapes

1. Accédez à **Authentification > Intégration > Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IdP Adapter**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à 'Credential Validators'**.
5. Sélectionnez [validateur d'identifiants de mot de passe](#) que vous avez créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonym**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si vous ne l'avez pas déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **Security > Signing & Decryption Keys & Certificates**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML que vous avez téléchargées depuis StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient de nombreuses valeurs spécifiques dont vous avez besoin.



Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID, afin que les utilisateurs puissent se connecter et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP. Ensuite, allez à [Créer des connexions SP supplémentaires](#) pour créer les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications > Integration > SP Connections**.
2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Import Metadata, sélectionnez **File**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé depuis la page Configure SSO pour le nœud d'administration.
3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

L'identifiant d'entité du partenaire et le nom de la connexion sont définis sur l'identifiant de connexion SP de 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 **Next**.

Configurer l'authentification unique (SSO) du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer le SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options **SSO initié par le SP**, **SLO initié par le SP**, **SSO initié par l'IdP** et **SLO initié par l'IdP**.
3. Sélectionnez **Next**.
4. Dans l'onglet Durée de vie de l'assertion, ne modifiez rien.
5. Dans l'onglet Création d'assertions, sélectionnez **Configurer la création d'assertions**.
 - 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 retirer la `urn:oid`, qui n'est pas utilisée.

Mapper l'instance d'adaptateur

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance d'adaptateur, sélectionnez [instance d'adaptateur](#) que vous avez créée.
3. Dans l'onglet Méthode de mappage, sélectionnez **Récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attributs et recherche d'utilisateurs, sélectionnez **Ajouter une source d'attributs**.
5. Dans l'onglet « Stockage de données », saisissez une description et sélectionnez l'élément [magasin de données](#) que vous avez ajouté.
6. Dans l'onglet Recherche dans l'annuaire LDAP :
 - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
 - Pour l'étendue de la recherche, sélectionnez **Sous-arbre**.
 - Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet Types d'encodage des attributs binaires LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=\${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez soit **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source des attributs.
11. Dans l'onglet Source de l'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Vérifiez le récapitulatif et sélectionnez **Terminé**.

13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet **SP Connection > Browser SSO > Protocol Settings**, sélectionnez **Configure Protocol Settings**.
2. Sur l'onglet URL du service de consommation d'assertion, acceptez les valeurs par défaut, qui ont été importées des métadonnées SAML de StorageGRID (**POST** pour la liaison et `/api/saml-response` pour l'URL du point de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées des métadonnées SAML de StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison).
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases à cocher **Require Authn Requests to be Signed** et **Always Sign Assertion** sélectionnées.
6. Dans l'onglet Encryption Policy, sélectionnez **None**.
7. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres Browser SSO.

Configurer les identifiants

Étapes

1. Dans l'onglet Connexion SP, sélectionnez **Informations d'identification**.
2. Dans l'onglet Identifiants, sélectionnez **Configurer les identifiants**.
3. Sélectionnez l'[certificat de signature](#) que vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **Manage Signature Verification Settings**.
 - a. Dans l'onglet Modèle de confiance, sélectionnez **Non ancré**.
 - b. Dans l'onglet Certificat de vérification de signature, vérifiez les informations du certificat de signature, qui ont été importées à partir des métadonnées SAML de StorageGRID.
5. Consultez les écrans récapitulatifs et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion SP pour créer les connexions SP nécessaires pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.



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

Étapes

1. Sélectionnez **Action > Copier** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Saisissez l'ID de connexion et le nom de la connexion pour la copie, puis sélectionnez **Enregistrer**.

3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
 - a. Sélectionnez **Action > Mettre à jour avec les métadonnées**.
 - b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.
 - c. Sélectionnez **Next**.
 - d. Sélectionnez **Enregistrer**.
4. Résolvez l'erreur due à l'attribut inutilisé :
 - a. Sélectionnez la nouvelle connexion.
 - b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > Contrat d'attributs**.
 - c. Supprimez l'entrée pour **urn:oid**.
 - d. Sélectionnez **Enregistrer**.

Désactiver SSO dans StorageGRID

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.

La page d'authentification unique s'affiche.

2. Sélectionnez **Désactiver l'authentification unique**.
3. Sélectionnez **Oui**.

Un message d'avertissement s'affiche, indiquant que les utilisateurs locaux pourront désormais se connecter.

La prochaine fois que vous vous connecterez à StorageGRID, la page de connexion StorageGRID s'affichera et vous devrez saisir le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique (SSO) pour un nœud d'administration StorageGRID

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

Avant de commencer

- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez le `Passwords.txt` fichier.

- Vous connaissez le mot de passe de l'utilisateur root local.

À propos de cette tâche

Après avoir désactivé l'authentification unique (SSO) pour un nœud d'administration, vous pouvez vous connecter au Grid Manager en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver l'authentification unique (SSO) sur le nœud d'administration dès que vous vous déconnectez.



La désactivation de l'authentification unique (SSO) pour un nœud d'administration n'affecte pas les paramètres SSO des autres nœuds d'administration de la grille. La case à cocher **Enable SSO** sur la page Single Sign-on dans le Grid Manager reste sélectionnée, et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
 - c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
 - d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

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

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

3. Confirmez que vous souhaitez désactiver SSO.

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

4. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.

La page de connexion de Grid Manager s'affiche désormais 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 temporairement l'authentification unique (SSO) parce que vous deviez corriger la configuration SSO :
 - a. Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
 - b. Modifiez les paramètres SSO incorrects ou obsolètes.
 - c. Sélectionnez **Enregistrer**.

La sélection de **Enregistrer** sur la page d'authentification unique réactive automatiquement l'authentification unique (SSO) pour l'ensemble de la grille.

7. Si vous avez désactivé temporairement l'authentification unique (SSO) parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :
 - a. Effectuez la ou les tâches que vous devez accomplir.
 - b. Sélectionnez **Se déconnecter**, puis fermez le Grid Manager.

c. Réactivez l'authentification unique (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 l'authentification unique (SSO).

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

- Redémarrez le nœud de grille : `reboot`

8. Depuis un navigateur Web, accédez au Grid Manager depuis le même nœud d'administration.

9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos identifiants SSO pour accéder au Grid Manager.

`${post_edited_translations.segment}`

Découvrez la fédération de grilles StorageGRID

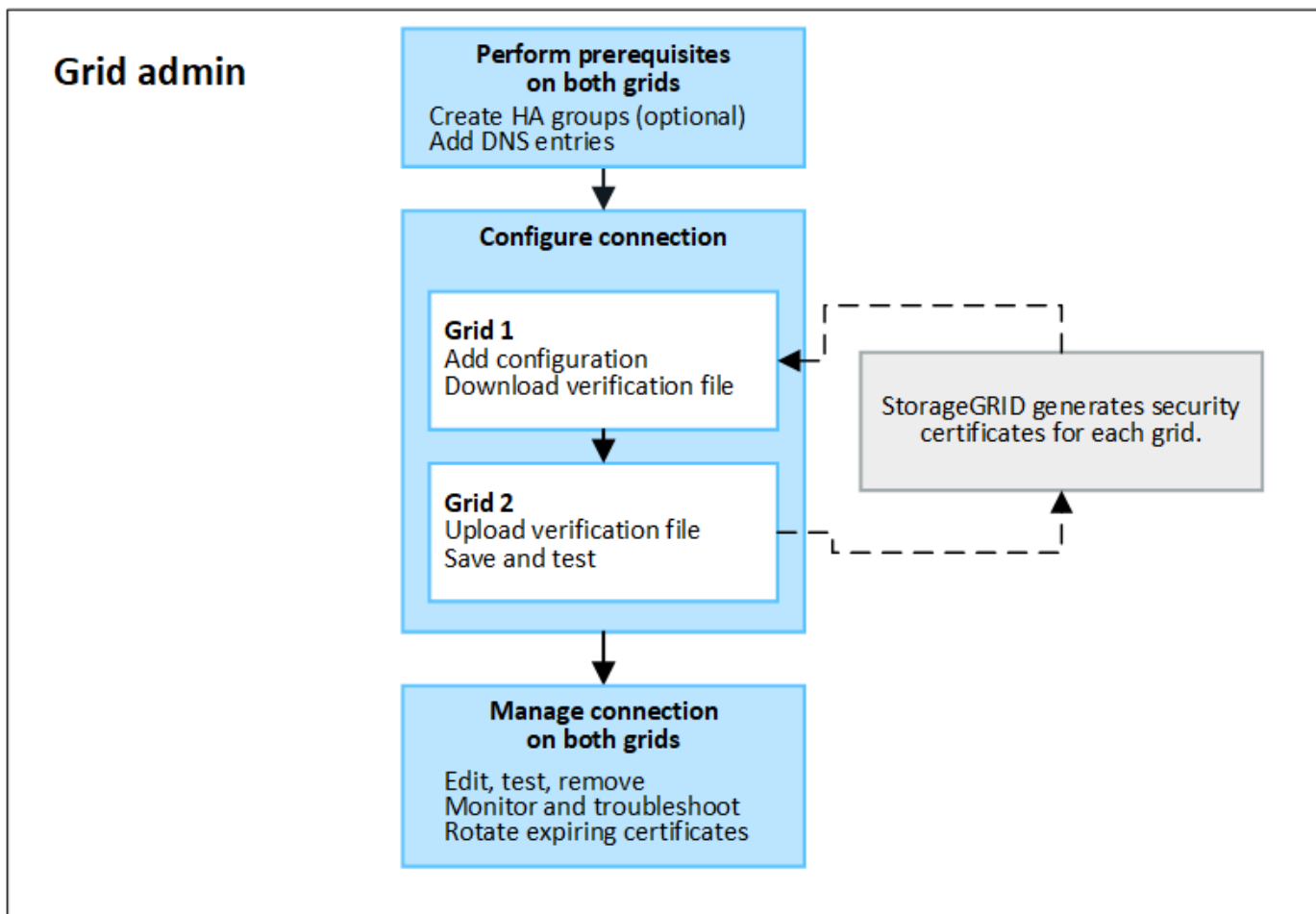
Vous pouvez utiliser la fédération de grilles pour cloner des locataires et répliquer leurs objets entre deux systèmes StorageGRID à des fins de reprise après sinistre.

Qu'est-ce qu'une connexion de fédération de grille ?

Une connexion de fédération de grille est une connexion bidirectionnelle, fiable et sécurisée entre les nœuds d'administration et les nœuds de passerelle dans deux systèmes StorageGRID.

Flux de travail pour la fédération de grid

Le diagramme de flux de travail résume les étapes de configuration d'une connexion de fédération de grilles entre deux grilles.



Considérations et exigences relatives aux connexions de fédération de grid

- Les grilles utilisées pour la fédération de grilles doivent exécuter des versions de StorageGRID qui sont soit identiques, soit présentant au maximum une différence d'une version majeure entre elles.

Pour plus de détails sur les exigences de version, consultez ["Notes de version"](#). Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

- Un grid peut avoir une ou plusieurs connexions de fédération avec d'autres grilles. Chaque connexion de fédération de grid est indépendante des autres connexions. Par exemple, si Grid 1 a une connexion avec Grid 2 et une seconde connexion avec Grid 3, il n'existe aucune connexion implicite entre Grid 2 et Grid 3.
- Les connexions de fédération de grilles sont bidirectionnelles. Une fois la connexion établie, vous pouvez surveiller et gérer la connexion depuis l'une ou l'autre grille.
- Au moins une connexion de fédération de grille doit exister avant que vous puissiez utiliser ["clone de compte"](#) ou ["réplication inter-grilles"](#).

Exigences en matière de réseau et d'adresse IP

- Les connexions de fédération de grilles peuvent s'effectuer sur le réseau de grille, le réseau d'administration ou le réseau client.
- Une connexion de fédération de grilles relie une grille à une autre grille. La configuration de chaque grille spécifie un point de terminaison de fédération de grille sur l'autre grille, composé de nœuds d'administration, de nœuds de passerelle ou des deux.
- La bonne pratique consiste à connecter ["groupes à haute disponibilité \(HA\)"](#) les nœuds Gateway et Admin

sur chaque grille. L'utilisation de groupes HA permet de garantir que les connexions de fédération de grille resteront en ligne si des nœuds deviennent indisponibles. Si l'interface active dans l'un ou l'autre groupe HA échoue, la connexion peut utiliser une interface de secours.

- Il est déconseillé d'établir une connexion de fédération de grille utilisant l'adresse IP d'un seul nœud d'administration ou nœud de passerelle. Si ce nœud devient indisponible, la connexion de fédération de grille le sera également.
- **"Réplication inter-grilles"** L'accès aux objets nécessite que les nœuds de stockage de chaque grille puissent accéder aux nœuds Admin et Gateway configurés sur l'autre grille. Pour chaque grille, confirmez que tous les nœuds de stockage disposent d'une route à large bande passante vers les nœuds Admin ou Gateway utilisés pour la connexion.

Utilisez les FQDN (Fully Qualified Domain Names) pour équilibrer la charge de la connexion.

Pour un environnement de production, utilisez des noms de domaine complets (FQDN) pour identifier chaque grille dans la connexion. Créez ensuite les entrées DNS appropriées, comme suit :

- Le nom de domaine complet (FQDN) de Grid 1 est mappé à une ou plusieurs adresses IP virtuelles (VIP) pour les groupes HA dans Grid 1 ou à l'adresse IP d'un ou plusieurs nœuds Admin ou Gateway dans Grid 1.
- Le nom de domaine complet (FQDN) de Grid 2 est associé à une ou plusieurs adresses VIP pour Grid 2 ou à l'adresse IP d'un ou plusieurs nœuds Admin ou Gateway dans Grid 2.

Lorsque vous utilisez plusieurs entrées DNS, les requêtes d'utilisation de la connexion sont réparties en charge, comme suit :

- Les entrées DNS qui correspondent aux adresses VIP de plusieurs groupes HA sont réparties entre les nœuds actifs des groupes HA.
- Les entrées DNS qui correspondent aux adresses IP de plusieurs nœuds d'administration ou nœuds de passerelle sont réparties entre les nœuds correspondants.

Exigences relatives aux ports

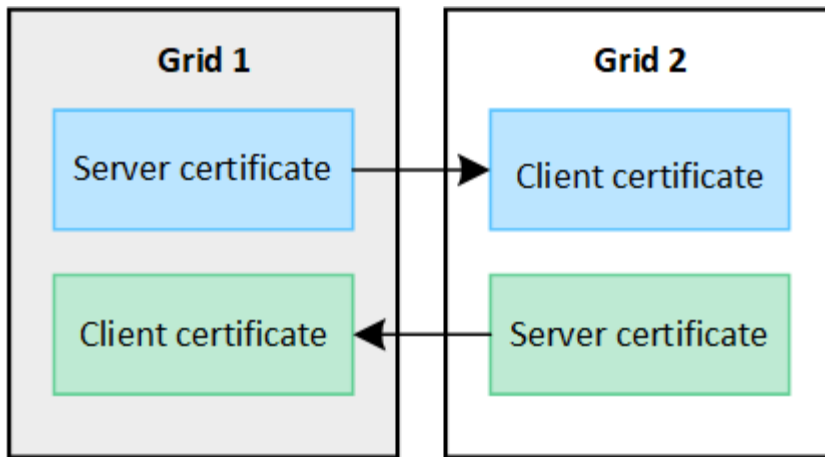
Lors de la création d'une connexion de fédération de grilles, vous pouvez spécifier n'importe quel numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utiliseront le même port.

Vous devez vous assurer qu'aucun nœud dans l'une ou l'autre grille n'utilise ce port pour d'autres connexions.

Exigences relatives aux certificats

Lorsque vous configurez une connexion de fédération de grille, StorageGRID génère automatiquement quatre certificats SSL :

- Certificats serveur et client pour authentifier et chiffrer les informations envoyées de la grille 1 à la grille 2
- Certificats serveur et client pour authentifier et chiffrer les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valides pendant 730 jours (2 ans). À l'approche de leur date d'expiration, l'alerte **Expiration of grid federation certificate** vous rappelle de renouveler les certificats, ce que vous pouvez faire à l'aide du Grid Manager.



Si les certificats des deux extrémités de la connexion expirent, la connexion cessera de fonctionner. La réplication des données sera en attente jusqu'à la mise à jour des certificats.

En savoir plus

- ["Créer des connexions de fédération de grille"](#)
- ["Gérer les connexions de fédération de grille"](#)
- ["Dépanner les erreurs de fédération de grille"](#)

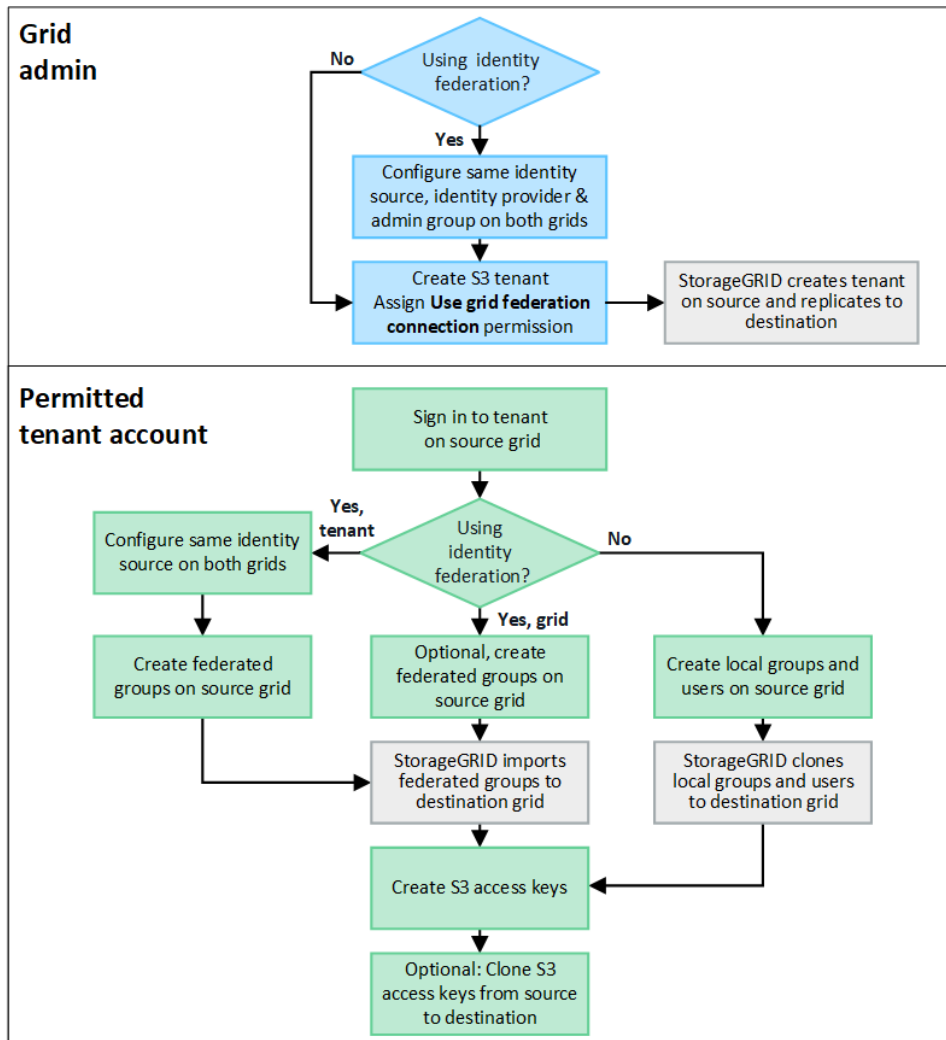
En savoir plus sur le clonage de compte dans StorageGRID

Le clonage de compte est la réplication automatique d'un compte locataire, de groupes de locataires, d'utilisateurs locataires et, éventuellement, de clés d'accès S3 entre les systèmes StorageGRID dans un ["connexion de fédération de grille"](#).

Le clonage de compte est nécessaire pour ["réplication inter-grilles"](#). Le clonage des informations de compte d'un système StorageGRID source vers un système StorageGRID de destination garantit que les utilisateurs et groupes locataires peuvent accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Flux de travail pour le clonage de compte

Le diagramme de flux de travail illustre les étapes que les administrateurs de grille et les locataires autorisés devront suivre pour configurer le clonage de compte. Ces étapes sont effectuées après le ["La connexion de fédération de grille est configurée"](#).



Flux de travail d'administration de la grille

Les étapes que les administrateurs de grille effectuent dépendent du fait que les systèmes StorageGRID dans le "[connexion de fédération de grille](#)" utilisent l'authentification unique (SSO) ou la fédération d'identités.

Configurer l'authentification unique pour le clonage de compte (facultatif)

Si l'un ou l'autre des systèmes StorageGRID de la connexion de fédération de grille utilise l'authentification unique (SSO), les deux grilles doivent utiliser SSO. Avant de créer les comptes de locataire pour la fédération de grille, les administrateurs des grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez la même source d'identité pour les deux grilles. Voir "[Utilisez la fédération d'identités](#)".
2. Configurez le même fournisseur d'identité SSO (IdP) pour les deux grilles. Voir "[Configurer l'authentification unique](#)".
3. "[Créez le même groupe d'administrateurs](#)" sur les deux grilles en important le même groupe fédéré.

Lors de la création du locataire, vous sélectionnerez ce groupe pour avoir l'autorisation d'accès Root initiale pour les comptes de locataire source et de destination.



Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant que vous ne créiez le locataire, le locataire n'est pas répliqué vers la destination.

Configurer la fédération d'identités au niveau de la grille pour account clone (facultatif)

Si l'un des systèmes StorageGRID utilise la fédération d'identités sans SSO, les deux grilles doivent utiliser la fédération d'identités. Avant de créer les comptes locataires pour la fédération de grilles, les administrateurs des grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez la même source d'identité pour les deux grilles. Voir ["Utilisez la fédération d'identités"](#).
2. En option, si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes locataires source et de destination, ["créez le même groupe d'administrateurs"](#) sur les deux grilles en important le même groupe fédéré.



Si vous attribuez l'autorisation d'accès racine à un groupe fédéré qui n'existe pas sur les deux grilles, le locataire n'est pas répliqué sur la grille de destination.

3. Si vous ne souhaitez pas qu'un groupe fédéré dispose de l'autorisation d'accès Root initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur Root local.

Créer un compte locataire S3 autorisé

Après avoir éventuellement configuré l'authentification unique (SSO) ou la fédération d'identités, un administrateur de grille effectue ces étapes pour déterminer quels locataires peuvent répliquer les objets du compartiment vers d'autres systèmes StorageGRID.

Étapes

1. Déterminez la grille que vous souhaitez utiliser comme grille source du locataire pour les opérations de clonage de compte.

La grille sur laquelle le locataire est initialement créé est appelée *grille source* du locataire. La grille sur laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

2. Sur cette grille, créez un nouveau compte locataire S3 ou modifiez un compte existant.
3. Attribuez l'autorisation **Utiliser la connexion de fédération de grille**.
4. Si le compte locataire doit gérer ses propres utilisateurs fédérés, attribuez-lui l'autorisation **Utiliser sa propre source d'identité**.

Si cette autorisation est accordée, les comptes des locataires source et de destination doivent configurer la même source d'identité avant de créer des groupes fédérés. Les groupes fédérés ajoutés au locataire source ne peuvent être clonés dans le locataire de destination que si les deux grilles utilisent la même source d'identité.

5. Sélectionnez une connexion de fédération de grille spécifique.
6. Enregistrez le locataire nouveau ou modifié.

Lorsqu'un nouveau locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille** est enregistré, StorageGRID crée automatiquement une réplique de ce locataire sur l'autre grille, comme suit :

- Les deux comptes locataires possèdent le même identifiant de compte, le même nom, le même quota

de stockage et les mêmes autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré disposant des autorisations d'accès racine pour le locataire, ce groupe est cloné dans le locataire de destination.
- Si vous avez sélectionné un utilisateur local disposant des droits d'accès Root pour le locataire, cet utilisateur est cloné dans le locataire de destination. Cependant, le mot de passe de cet utilisateur n'est pas cloné.

Pour plus de détails, consultez ["Gérer les locataires autorisés pour la fédération de grilles"](#).

Flux de travail des comptes de locataire autorisé

Une fois qu'un locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille** est répliqué sur la grille de destination, les comptes locataires autorisés peuvent effectuer ces étapes pour cloner les groupes de locataires, les utilisateurs et les clés d'accès S3.

Étapes

1. Connectez-vous au compte locataire sur la grille source du locataire.
2. Si cela est autorisé, configurez la fédération d'identité sur les comptes locataires source et de destination.
3. Créez des groupes et des utilisateurs sur le tenant source.

Lorsque de nouveaux groupes ou utilisateurs sont créés sur le locataire source, StorageGRID les clone automatiquement sur le locataire de destination, mais aucun clonage n'a lieu de la destination vers la source.

4. Créez des clés d'accès S3.
5. Vous pouvez, si vous le souhaitez, cloner les clés d'accès S3 du locataire source vers le locataire de destination.

Pour plus de détails sur le flux de travail des comptes locataires autorisés et pour savoir comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés, consultez ["Cloner les groupes de locataires et les utilisateurs"](#) et ["Cloner les clés d'accès S3 à l'aide de l'API"](#).

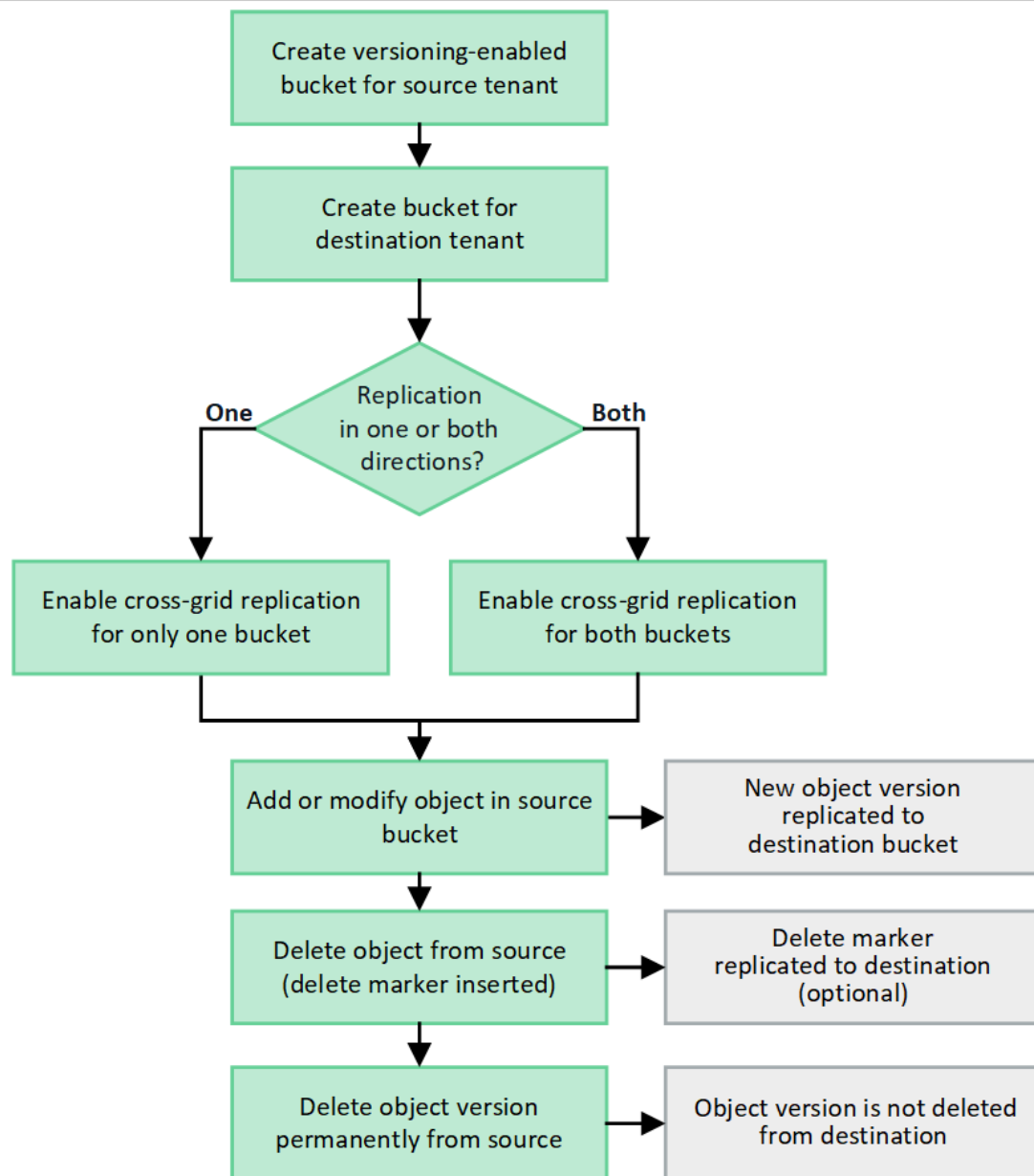
Découvrez la réplication inter-grilles dans StorageGRID

La réplication inter-grilles est la réplication automatique d'objets entre des compartiments S3 sélectionnés dans deux systèmes StorageGRID connectés dans un ["connexion de fédération de grille"](#). ["Clonage de compte"](#) est requis pour la réplication inter-grilles.

Flux de travail pour la réplication inter-grilles

Le diagramme de flux de travail résume les étapes de configuration de la réplication inter-grilles entre les compartiments sur deux grilles.

Tenant user



Exigences pour la réplication inter-grilles

Si un compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** pour utiliser une ou plusieurs "[connexions de fédération de grille](#)", un utilisateur locataire disposant d'une autorisation d'accès Root peut créer des compartiments dans les comptes locataires correspondants sur chaque grille. Ces compartiments :

- Peuvent avoir des noms différents l'un de l'autre
- Peut avoir différentes régions
- La gestion des versions doit être activée
- Doit être vide

Une fois les deux compartiments créés, la réplication inter-grilles peut être configurée pour l'un ou les deux compartiments.

En savoir plus

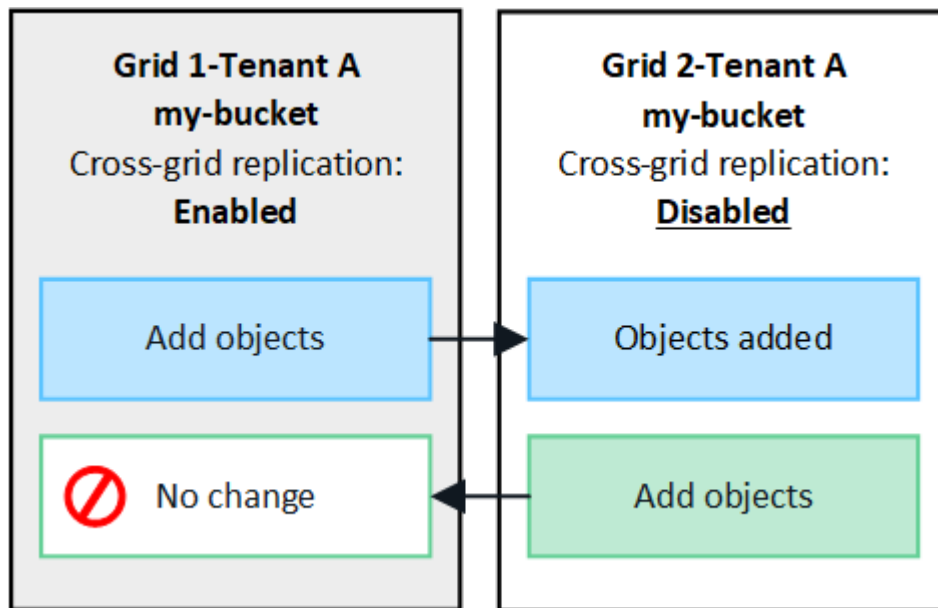
"Gérer la réplication inter-grilles"

Comment fonctionne la réplication inter-grilles

Vous pouvez configurer la réplication inter-grilles pour qu'elle s'effectue dans un seul sens ou dans les deux sens.

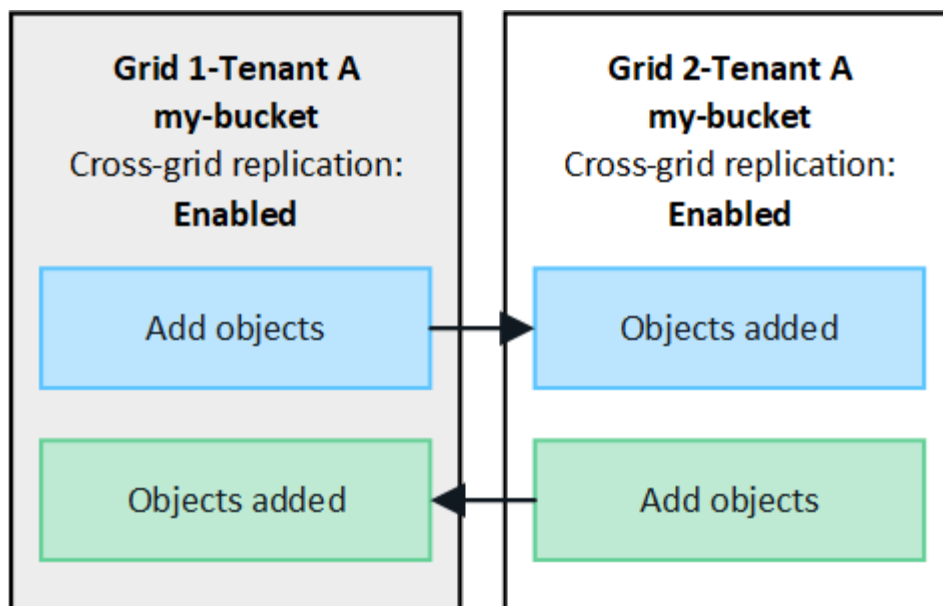
Réplication dans un seul sens

Si vous activez la réplication inter-grilles pour un compartiment sur une seule grille, les objets ajoutés à ce compartiment (le compartiment source) sont répliqués dans le compartiment correspondant sur l'autre grille (le compartiment de destination). Cependant, les objets ajoutés au compartiment de destination ne sont pas répliqués vers la source. Sur la figure, la réplication inter-grilles est activée pour `my-bucket` la grille 1 vers la grille 2, mais elle n'est pas activée dans l'autre sens.



Réplication dans les deux sens

Si vous activez la réplication inter-grilles pour un même compartiment sur les deux grilles, les objets ajoutés à l'un des compartiments sont répliqués sur l'autre grille. Sur la figure, la réplication inter-grilles est activée pour `my-bucket` dans les deux sens.



Que se passe-t-il lorsque des objets sont ingérés ?

Lorsqu'un client S3 ajoute un objet à un compartiment pour lequel la réplication inter-grilles est activée, le processus suivant se déroule :

1. StorageGRID réplique automatiquement l'objet du compartiment source vers le compartiment de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, notamment du nombre d'autres opérations de réplication en attente.

Le client S3 peut vérifier l'état de réplication d'un objet en envoyant une requête `GetObject` ou `HeadObject`. La réponse inclut un en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui prend l'une des valeurs suivantes :

Grid	État de la réplication
Source	• TERMINÉ : La réplication a réussi pour toutes les connexions au grid. • EN ATTENTE : L'objet n'a pas été répliqué vers au moins une connexion grid. • ÉCHEC : Aucune réplication n'est en attente pour aucune connexion au grid et au moins une a échoué avec une défaillance permanente. Un utilisateur doit résoudre l'erreur.
Destination	REPLICA : L'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge l'en-tête ``x-amz-replication-status``.

2. StorageGRID utilise les politiques ILM actives de chaque grille pour gérer les objets, comme n'importe quel autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservé indéfiniment, tandis que la copie de l'objet A répliquée sur la grille 2 peut être stockée avec un code d'effacement 2+1 et supprimée après trois ans.

Que se passe-t-il lorsque des objets sont supprimés ?

Comme décrit dans ["Supprimer le flux de données"](#), StorageGRID peut supprimer un objet pour l'une des raisons suivantes :

- Le client S3 émet une requête de suppression.
- Un utilisateur de Tenant Manager sélectionne l'"[Supprimer les objets dans le compartiment](#)" option pour supprimer tous les objets d'un compartiment.
- Le compartiment possède une configuration de cycle de vie, qui expire.
- La dernière période définie dans la règle ILM pour l'objet arrive à son terme, et aucun autre placement n'est spécifié.

Lorsqu'un objet StorageGRID est supprimé en raison d'une opération de suppression d'objets dans un compartiment, de l'expiration du cycle de vie du compartiment ou de l'expiration du placement ILM, l'objet répliqué n'est jamais supprimé de l'autre grille dans une connexion de fédération de grilles. Cependant, les marqueurs de suppression ajoutés au compartiment source par des suppressions effectuées par le client S3 peuvent, en option, être répliqués vers le compartiment de destination.

Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un compartiment dont la réplication inter-grilles est activée, examinez comment les clients S3 suppriment des objets des compartiments dont le versionnage est activé, comme suit :

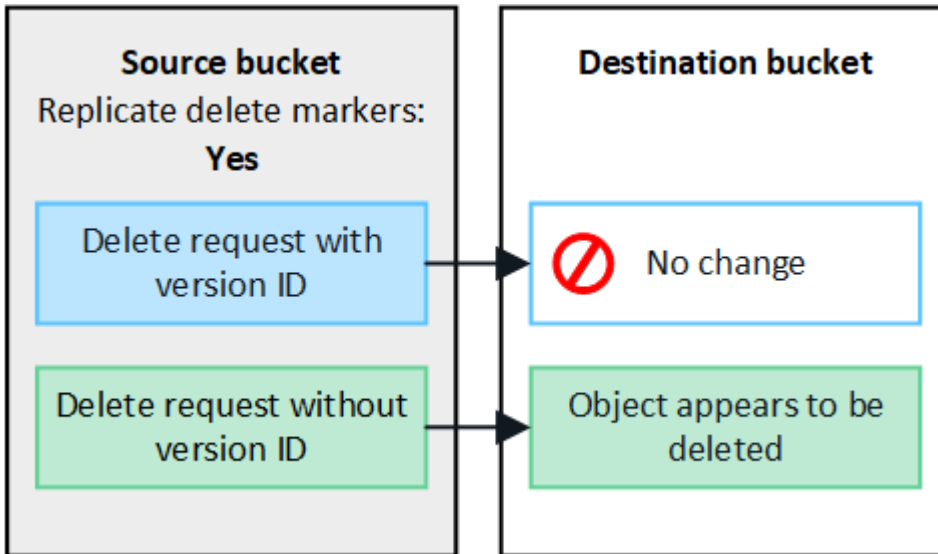
- Si un client S3 émet une requête de suppression incluant un ID de version, cette version de l'objet est définitivement supprimée. Aucun marqueur de suppression n'est ajouté au compartiment.
- Si un client S3 émet une requête de suppression sans inclure d'ID de version, StorageGRID ne supprime aucune version d'objet. À la place, il ajoute un marqueur de suppression au compartiment. Le marqueur de suppression fait en sorte que StorageGRID agisse comme si l'objet avait été supprimé :
 - Une requête `GetObject` sans identifiant de version échoue avec `404 No Object Found`
 - Une requête `GetObject` avec un ID de version valide aboutit et renvoie la version de l'objet demandée.

Lorsqu'un client S3 supprime un objet d'un compartiment sur lequel la réplication inter-grilles est activée, StorageGRID détermine s'il faut répliquer la requête de suppression vers la destination, comme suit :

- Si la requête de suppression inclut un identifiant de version, cette version de l'objet est définitivement supprimée de la grille source. Cependant, StorageGRID ne réplique pas les requêtes de suppression qui incluent un identifiant de version, de sorte que la même version de l'objet n'est pas supprimée de la destination.
- Si la demande de suppression ne contient pas d'identifiant de version, StorageGRID peut éventuellement répliquer le marqueur de suppression, en fonction de la configuration de la réplication inter-grilles pour le compartiment :
 - Si vous choisissez de répliquer les marqueurs de suppression (option par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment de destination. En conséquence, l'objet apparaît comme supprimé sur les deux grilles.
 - Si vous choisissez de ne pas répliquer les marqueurs de suppression, un marqueur de suppression est ajouté au compartiment source mais n'est pas répliqué dans le compartiment de destination. En conséquence, les objets supprimés sur la grille source ne sont pas supprimés sur la grille de destination.

Dans la figure, **Répliquer les marqueurs de suppression** était défini sur **Oui** lorsque ["La réplication inter-grilles a été activée"](#). Les requêtes de suppression pour le compartiment source qui incluent un ID de version ne suppriment pas les objets du compartiment de destination. Les requêtes de suppression pour le

compartiment source qui n'incluent pas d'ID de version semblent supprimer les objets du compartiment de destination.



Si vous souhaitez que les suppressions d'objets restent synchronisées entre les grilles, créez des ["Configurations du cycle de vie S3"](#) correspondants pour les compartiments sur les deux grilles.

Comment les objets chiffrés sont répliqués

Lorsque vous utilisez la réplication inter-grilles pour répliquer des objets entre des grilles, vous pouvez chiffrer des objets individuellement, utiliser le chiffrement par défaut du compartiment ou configurer le chiffrement à l'échelle de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement par défaut du compartiment ou de la grille avant ou après avoir activé la réplication inter-grilles pour un compartiment.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID) lors de l'ajout des objets au compartiment source. Utilisez l'`x-amz-server-side-encryption` en-tête de requête et spécifiez `AES256`. Voir ["Utilisez le chiffrement côté serveur"](#).



L'utilisation de SSE-C (chiffrement côté serveur avec des clés fournies par le client) n'est pas prise en charge pour la réplication inter-grilles. L'opération d'ingestion échouera.

Pour utiliser le chiffrement par défaut pour un compartiment, utilisez une requête `PutBucketEncryption` et définissez le paramètre `SSEAlgorithm` sur `AES256`. Le chiffrement au niveau du compartiment s'applique à tous les objets ingérés sans l'en-tête de requête `x-amz-server-side-encryption`. Voir ["Opérations sur les compartiments"](#).

Pour utiliser le chiffrement au niveau du grid, définissez l'option **Chiffrement des objets stockés** sur **AES-256**. Le chiffrement au niveau du grid s'applique à tous les objets qui ne sont pas chiffrés au niveau du compartiment ou qui sont ingérés sans l'en-tête de requête `x-amz-server-side-encryption`. Voir ["Configurer les options de réseau et d'objet"](#).



SSE ne prend pas en charge AES-128. Si l'option **Chiffrement des objets stockés** est activée pour la grille source avec l'option **AES-128**, l'utilisation de l'algorithme AES-128 n'est pas propagée à l'objet répliqué. À la place, l'objet répliqué utilise le paramètre de chiffrement par défaut du compartiment ou de la grille de destination, si disponible.

Pour déterminer comment chiffrer les objets sources, StorageGRID applique les règles suivantes :

1. Utilisez l'`x-amz-server-side-encryption` en-tête d'ingestion, s'il est présent.
2. Si aucun en-tête d'ingestion n'est présent, utilisez le paramètre de chiffrement par défaut du compartiment, s'il est configuré.
3. Si aucun paramètre de compartiment n'est configuré, utilisez le paramètre de chiffrement global de la grille, s'il est configuré.
4. Si aucun paramètre global n'est présent, ne chiffrez pas l'objet source.

Pour déterminer comment chiffrer les objets répliqués, StorageGRID applique ces règles dans cet ordre :

1. Utilisez le même chiffrement que l'objet source, sauf si cet objet utilise le chiffrement AES-128.
2. Si l'objet source n'est pas chiffré ou s'il utilise AES-128, utilisez le paramètre de chiffrement par défaut du compartiment de destination, s'il est configuré.
3. Si le compartiment de destination ne dispose pas d'un paramètre de chiffrement, utilisez le paramètre de chiffrement global de la grille de destination, s'il est configuré.
4. Si aucun paramètre global n'est présent, ne chiffrez pas l'objet de destination.

Réplication inter-grilles avec S3 Object Lock

Vous pouvez configurer la réplication inter-grilles entre les compartiments StorageGRID avec le verrouillage d'objet S3 activé dans les circonstances suivantes.

Lorsque le verrouillage d'objet S3 sur le compartiment source est...	Et le verrouillage d'objet S3 sur le compartiment de destination est...
Activé	Activé
Désactivées	Activé

Lorsque le verrouillage d'objet S3 sur le compartiment source est activé :

- Les objets sont verrouillés avec des paramètres de rétention à destination dans cet ordre :
 - a. Les valeurs d'en-tête de rétention de l'objet source pour :

`x-amz-object-lock-mode`
`x-amz-object-lock-retain-until-date`
 - b. Durée de rétention par défaut du compartiment source, si elle est définie.
 - c. La durée de rétention par défaut du compartiment de destination, si elle est définie.

La durée de rétention par défaut du compartiment de destination ne remplace pas les paramètres de rétention répliqués à partir de l'objet source.

- Vous pouvez définir le statut de rétention légale de l'objet de destination en utilisant `x-amz-object-lock-legal-hold` lors du chargement de l'objet.
- Une erreur se produit si le locataire ou le compartiment de destination ne prend pas en charge les paramètres de S3 Object Lock de l'objet source. Consultez ["Alertes et erreurs de réplication inter-grilles."](#)

Lorsque le verrouillage d'objet S3 sur le compartiment source est désactivé :

- Vous pouvez configurer la rétention par défaut sur le compartiment de destination pour appliquer les paramètres de rétention S3 Object Lock à l'objet de destination.
- L'objet de destination ne peut pas définir de statut de rétention légale.

PutObjectTagging et DeleteObjectTagging ne sont pas pris en charge

PutObjectTagging et DeleteObjectTagging ne sont pas prises en charge pour les objets dans des compartiments ayant la réplication inter-grilles activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, 501 Not Implemented est renvoyé. Le message est Put (Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.

PutObjectRetention et PutObjectLegalHold ne sont pas pris en charge

PutObjectRetention et PutObjectLegalHold ne sont pas entièrement prises en charge pour les objets dans des compartiments ayant la réplication inter-grilles activée.

Si un client S3 émet une requête PutObjectRetention ou une requête PutObjectLegalHold, les paramètres de l'objet source sont modifiés, mais les modifications ne sont pas appliquées à la destination.

Comment les objets segmentés sont répliqués

La taille maximale des segments de la grille source s'applique aux objets répliqués vers la grille de destination. Lorsque des objets sont répliqués vers une autre grille, le paramètre **Taille maximale des segments (Configuration > Système > Options de stockage)** de la grille source est utilisé sur les deux grilles. Par exemple, supposons que la taille maximale des segments de la grille source soit de 1 Go, tandis que la taille maximale des segments de la grille de destination soit de 50 Mo. Si vous ingérez un objet de 2 Go sur la grille source, cet objet est enregistré en deux segments de 1 Go. Il est également répliqué vers la grille de destination en deux segments de 1 Go, même si la taille maximale des segments de cette grille est de 50 Mo.

Comparer la réplication inter-grilles et la réplication CloudMirror dans StorageGRID

Lorsque vous commencez à utiliser la fédération de grilles, examinez les similitudes et les différences entre "[réplication inter-grilles](#)" et le "[Service de réplication CloudMirror StorageGRID](#)".



Vous ne pouvez pas utiliser CloudMirror sur un bucket répliqué par réplication inter-grilles, et inversement.

	Réplication inter-grilles	CloudMirror service de réplication
Quel est l'objectif principal ?	Un système StorageGRID fait office de système de reprise après sinistre. Les objets d'un bucket peuvent être répliqués entre les grilles dans un sens ou dans les deux sens.	Permet à un locataire de répliquer automatiquement des objets d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). CloudMirror replication crée une copie indépendante d'un objet dans une infrastructure S3 indépendante. Cette copie indépendante n'est pas utilisée comme sauvegarde, mais est souvent traitée ultérieurement dans le cloud.
Comment est-ce configuré ?	1. Configurez une connexion de fédération de grilles entre deux grilles. 2. Ajoutez de nouveaux comptes locataires, qui sont automatiquement clonés sur l'autre grille. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs, qui sont également clonés. 4. Créez des compartiments correspondants sur chaque grille et activez la réplication inter-grilles dans un sens ou dans les deux sens.	1. Un utilisateur locataire configure la réplication CloudMirror en définissant un point de terminaison CloudMirror (adresse IP, informations d'identification, etc.) à l'aide du Tenant Manager ou de l'API S3. 2. Tout compartiment appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.
Qui est responsable de sa mise en place ?	• Un administrateur de grille configure la connexion et les tenants. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les compartiments.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un compartiment S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération de grille.	• Toute infrastructure S3 compatible (y compris Amazon S3). • Google Cloud Platform (GCP)
Le versionnage des objets est-il nécessaire ?	Oui, les compartiments source et de destination doivent tous deux avoir le versionnage des objets activé.	Non, la réplication CloudMirror prend en charge toute combinaison de compartiments non versionnés et versionnés, aussi bien à la source qu'à la destination.

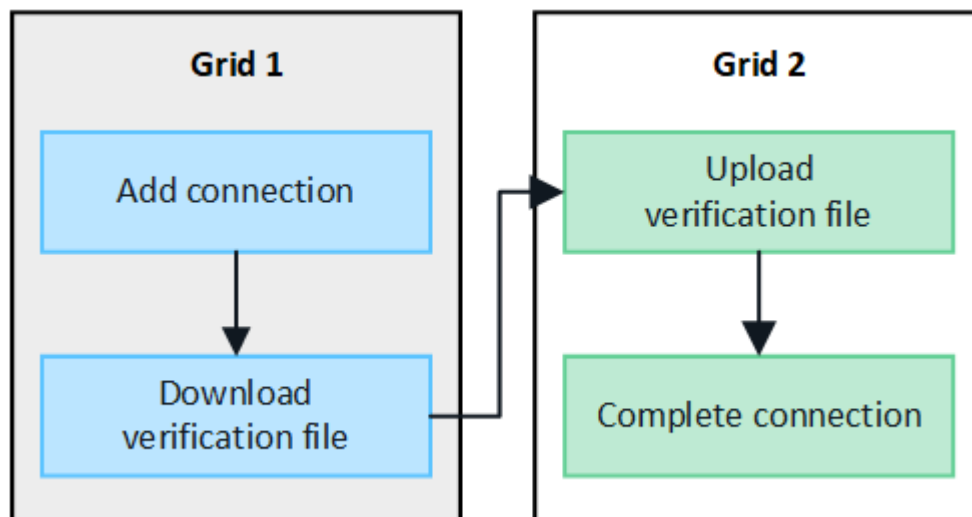
	Réplication inter-grilles	CloudMirror service de réplication
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment qui a la réplication inter-grilles activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment configuré avec un point de terminaison CloudMirror. Les objets présents dans le compartiment source avant que ce dernier ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grilles crée des objets versionnés et réplique l'identifiant de version du compartiment source vers le compartiment de destination. Cela permet de conserver l'ordre des versions entre les deux grilles.	CloudMirror replication ne nécessite pas de compartiments avec versionnage activé, donc CloudMirror ne peut maintenir l'ordre d'une clé qu'au sein d'un site. Il n'y a aucune garantie que l'ordre sera maintenu pour les requêtes adressées à un objet sur un site différent.
Que se passe-t-il si un objet ne peut pas être répliqué ?	L'objet est mis en file d'attente pour réplication, sous réserve des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de la plateforme (voir "Recommandations pour l'utilisation des services de la plateforme").
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, ses métadonnées système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non, lorsqu'un objet est répliqué dans le compartiment externe, ses métadonnées système sont mises à jour. Les métadonnées diffèrent selon l'emplacement, en fonction de l'heure d'ingestion et du comportement de l'infrastructure S3 indépendante.
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire des objets en effectuant une requête auprès du compartiment sur l'une ou l'autre grille.	Les applications peuvent récupérer ou lire des objets en effectuant une requête auprès de StorageGRID ou de la destination S3. Par exemple, supposons que vous utilisez la réplication CloudMirror pour dupliquer des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour des objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.

	Réplication inter-grilles	CloudMirror service de réplication
Que se passe-t-il si un objet est supprimé ?	- Les demandes de suppression incluant un ID de version ne sont jamais répliquées vers la grille de destination. - Les demandes de suppression qui n'incluent pas d'identifiant de version ajoutent un marqueur de suppression au compartiment source, qui peut éventuellement être répliqué vers la grille de destination. - Si la réplication inter-grille est configurée dans un seul sens, les objets du compartiment de destination peuvent être supprimés sans affecter la source.	Les résultats varieront en fonction de l'état de version des compartiments source et de destination (qui n'ont pas besoin d'être identiques) : - Si les deux compartiments sont versionnés, une demande de suppression ajoutera un marqueur de suppression dans les deux emplacements. - Si seul le compartiment source est versionné, une requête de suppression ajoutera un marqueur de suppression à la source mais pas à la destination. - Si aucun des deux compartiments n'est versionné, une requête de suppression supprimera l'objet de la source mais pas de la destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.

Créer des connexions de fédération de grille StorageGRID

Vous pouvez créer une connexion de fédération de grilles entre deux systèmes StorageGRID si vous souhaitez cloner les détails du locataire et répliquer les données des objets.

Comme illustré, la création d'une connexion de fédération de grilles nécessite des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la complétez sur l'autre grille. Vous pouvez commencer à partir de l'une ou l'autre grille.



Avant de commencer

- Vous avez examiné la "[considérations et exigences](#)" pour la configuration des connexions de fédération de grille.
- Si vous prévoyez d'utiliser des noms de domaine complets (FQDN) pour chaque grille au lieu d'adresses IP ou VIP, vous savez quels noms utiliser et vous avez confirmé que le serveur DNS de chaque grille possède les entrées appropriées.
- Vous utilisez un "[navigateur Web pris en charge](#)".
- Vous disposez des droits d'accès Root et de la phrase secrète de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un ou l'autre des deux systèmes StorageGRID.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez **Ajouter une connexion**.
4. Saisissez les détails de la connexion.

Champ	Description
Nom de la connexion	Un nom unique pour vous aider à reconnaître cette connexion, par exemple, « Grid 1-Grid 2 ».
FQDN ou adresse IP pour cette grille	L'un des éléments suivants : • Le nom de domaine complet (FQDN) de la grille à laquelle vous êtes actuellement connecté • Adresse VIP d'un groupe HA sur cette grille • Adresse IP d'un nœud d'administration ou d'un nœud passerelle sur cette grille. L'adresse IP peut être sur n'importe quel réseau que la grille de destination peut atteindre.
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez saisir n'importe quel numéro de port inutilisé entre 23000 et 23999. Les deux grilles de cette connexion utiliseront le même port. Vous devez vous assurer qu'aucun nœud dans l'une ou l'autre grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Le nombre de jours pendant lesquels vous souhaitez que les certificats de sécurité pour cette grille dans la connexion soient valides. La valeur par défaut est de 730 jours (2 ans), mais vous pouvez saisir une valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.

Champ	Description
Phrase secrète de provisionnement pour cette grille	La phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
FQDN ou adresse IP pour l'autre grid	L'un des éléments suivants : • Le domaine complet (FQDN) de la grille à laquelle vous souhaitez vous connecter • Une adresse VIP d'un groupe HA sur l'autre grille • Adresse IP d'un nœud d'administration ou d'un nœud passerelle sur l'autre grille. L'adresse IP peut être sur n'importe quel réseau que la grille source peut atteindre.

5. Sélectionnez **Enregistrer et continuer**.

6. Pour l'étape Télécharger le fichier de vérification, sélectionnez **Télécharger le fichier de vérification**.

Une fois la connexion établie sur l'autre grid, vous ne pourrez plus télécharger le fichier de vérification depuis aucun des deux grids.

7. Localisez le fichier téléchargé (*connection-name.grid-federation*, puis enregistrez-le dans un emplacement sûr.



Ce fichier contient des secrets (masqués comme *****) et d'autres informations sensibles et doit être stocké et transmis en toute sécurité.

8. Sélectionnez **Fermer** pour revenir à la page de fédération Grid.

9. Vérifiez que la nouvelle connexion est affichée et que son **statut de connexion** est **En attente de connexion**.

10. Transmettez le *connection-name.grid-federation* fichier à l'administrateur de l'autre grille.

Connexion complète

Effectuez ces étapes sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez **Téléverser un fichier de vérification** pour accéder à la page de téléversement.
4. Sélectionnez **Téléverser le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé depuis la première grille (*connection-name.grid-federation*).

Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours de validité pour les certificats de sécurité de cette grille. Le champ **Durée de validité du certificat** reprend par défaut la valeur saisie dans la première grille, mais chaque grille peut utiliser une date d'expiration différente.

En règle générale, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.



Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les répliquions seront en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase secrète de provisionnement de la grille à laquelle vous êtes actuellement connecté.

7. Sélectionnez **Enregistrer et tester**.

Les certificats sont générés et la connexion est testée. Si la connexion est valide, un message de confirmation s'affiche et la nouvelle connexion est répertoriée sur la page de fédération Grid. L'état de la connexion sera **Connecté**.

Si un message d'erreur apparaît, corrigez les problèmes rencontrés. Voir "[Dépanner les erreurs de fédération de grille](#)".

8. Accédez à la page de fédération de grilles de la première grille et actualisez le navigateur. Confirmez que l'état de la connexion est maintenant « Connecté ».

9. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier d'origine ne pourra pas être réutilisé.

Après avoir terminé

- Examinez les éléments à prendre en compte pour "[gestion des locataires autorisés](#)".
- "[Créez un ou plusieurs nouveaux comptes locataires](#)", attribuez l'autorisation **Utiliser la connexion de fédération de grille** et sélectionnez la nouvelle connexion.
- "[Gérer la connexion](#)" si nécessaire. Vous pouvez modifier les valeurs de connexion, tester une connexion, renouveler les certificats de connexion ou supprimer une connexion.
- "[Surveillez la connexion](#)" dans le cadre de vos activités habituelles de surveillance StorageGRID.
- "[Résoudre les problèmes de connexion](#)", y compris la résolution de toute alerte et erreur liée au clonage de compte et à la répliquion inter-grilles.

Gérer les connexions de fédération de grille StorageGRID

La gestion des connexions de fédération de grilles entre les systèmes StorageGRID comprend la modification des détails de connexion, la rotation des certificats, la suppression des autorisations des locataires et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous disposez des "[Autorisation d'accès root](#)" pour la grille à laquelle vous êtes connecté.

Modifier une connexion de fédération de grille

Vous pouvez modifier une connexion de fédération de grilles en vous connectant au nœud d'administration principal de l'une ou l'autre grille de la connexion. Après avoir effectué des modifications sur la première grille, vous devez télécharger un nouveau fichier de vérification et le téléverser sur l'autre grille.



Pendant la modification de la connexion, les demandes de clonage de compte ou de réplication entre grilles continueront d'utiliser les paramètres de connexion existants. Les modifications que vous apportez à la première grille sont enregistrées localement, mais ne sont utilisées qu'une fois qu'elles ont été téléchargées vers la seconde grille, enregistrées et testées.

Commencez à modifier la connexion

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Nœuds** et vérifiez que tous les autres Admin Nodes de votre système sont en ligne.



Lorsque vous modifiez une connexion de fédération de grilles, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, un message d'avertissement s'affiche lorsque vous sélectionnez **Enregistrer et tester**.

3. Sélectionnez **Configuration > System > Grid federation**.
4. Modifiez les détails de la connexion à l'aide du menu **Actions** sur la page de fédération Grid ou sur la page de détails d'une connexion spécifique. Consultez "[Créer des connexions de fédération de grille](#)" pour savoir quoi saisir.

Menu Actions

- a. Sélectionnez le bouton radio pour la connexion.
- b. Sélectionnez **Actions > Modifier**.
- c. Saisissez les nouvelles informations.

Page de détails

- a. Sélectionnez un nom de connexion pour afficher ses détails.
- b. Sélectionnez **Modifier**.
- c. Saisissez les nouvelles informations.

5. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
6. Sélectionnez **Enregistrer et continuer**.

Les nouvelles valeurs sont enregistrées, mais elles ne seront appliquées à la connexion que lorsque vous aurez téléchargé le nouveau fichier de vérification sur l'autre grid.

7. Sélectionnez **Télécharger le fichier de vérification**.

Pour télécharger ce fichier ultérieurement, rendez-vous sur la page de détails de la connexion.

8. Localisez le fichier téléchargé (`connection-name.grid-federation`), puis enregistrez-le dans un emplacement sûr.



Le fichier de vérification contient des informations confidentielles et doit être stocké et transmis de manière sécurisée.

9. Sélectionnez **Fermer** pour revenir à la page de fédération Grid.
10. Confirmez que l'état de la connexion est « En attente de modification ».



Si l'état de la connexion était autre que **Connecté** lorsque vous avez commencé à modifier la connexion, il ne passera pas à **Modification en attente**.

11. Transmettez le `connection-name.grid-federation` fichier à l'administrateur de l'autre grille.

Terminez la modification de la connexion

Terminez la modification de la connexion en téléchargeant le fichier de vérification sur l'autre grid.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez **Téléverser le fichier de vérification** pour accéder à la page de téléversement.
4. Sélectionnez **Téléverser le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé depuis la première grille.
5. Saisissez la phrase secrète de provisionnement de la grille à laquelle vous êtes actuellement connecté.
6. Sélectionnez **Enregistrer et tester**.

Si la connexion peut être établie avec les valeurs modifiées, un message de confirmation s'affiche. Sinon, un message d'erreur s'affiche. Examinez le message et résolvez tout problème.
7. Fermez l'assistant pour revenir à la page de fédération Grid.
8. Confirmez que l'état de la **connexion** est **Connecté**.
9. Accédez à la page de fédération de grilles de la première grille et actualisez le navigateur. Confirmez que l'état de la connexion est maintenant « Connecté ».
10. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Tester une connexion de fédération de grille

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Testez la connexion à l'aide du menu **Actions** sur la page de fédération Grid ou sur la page de détails d'une connexion spécifique.

Menu Actions

- a. Sélectionnez le bouton radio pour la connexion.
- b. Sélectionnez **Actions > Test**.

Page de détails

- a. Sélectionnez un nom de connexion pour afficher ses détails.
- b. Sélectionnez **Test connection**.

4. Vérifiez l'état de la connexion :

État de la connexion	Description
Connecté	Les deux grids sont connectés et communiquent normalement.
Erreur	La connexion est en état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
En attente de modification	Vous avez modifié la connexion sur cette grille, mais celle-ci utilise toujours la configuration existante. Pour finaliser la modification, téléversez le nouveau fichier de vérification sur l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais celle-ci n'est pas encore établie sur l'autre grille. Téléchargez le fichier de vérification depuis cette grille et chargez-le sur l'autre grille.
Inconnu	La connexion est dans un état inconnu, probablement en raison d'un problème de réseau ou d'un nœud hors ligne.

5. Si l'état de la connexion est **Erreur**, résolvez tout problème. Ensuite, sélectionnez à nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

Rotation des certificats de connexion

Chaque connexion de fédération de grilles utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille approchent de leur date d'expiration, l'alerte **Expiration of grid federation certificate** vous rappelle de renouveler les certificats.



Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les répliques seront en attente jusqu'à ce que les certificats soient mis à jour.

Étapes

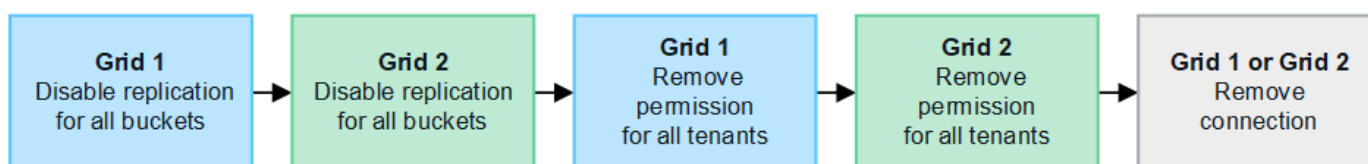
1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Depuis l'un ou l'autre onglet de la page de fédération Grid, sélectionnez le nom de la connexion pour afficher ses détails.

4. Sélectionnez l'onglet **Certificats**.
5. Sélectionnez **Faire pivoter les certificats**.
6. Indiquez combien de jours les nouveaux certificats doivent être valides.
7. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
8. Sélectionnez **Faire pivoter les certificats**.
9. Si nécessaire, répétez ces étapes sur l'autre grille de la connexion.

En règle générale, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

Supprimer une connexion de fédération de grille

Vous pouvez supprimer une connexion de fédération de grilles depuis l'une ou l'autre des grilles. Comme illustré, vous devez effectuer les étapes préalables sur les deux grilles pour vérifier que la connexion n'est utilisée par aucun locataire sur l'une ou l'autre des grilles.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime pas les éléments déjà copiés entre les grilles. Par exemple, les utilisateurs, groupes et objets du locataire présents dans les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, tous les objets en attente de répllication (ingérés mais pas encore répliqués sur l'autre grille) verront leur répllication définitivement échouer.

Désactivez la répllication pour tous les compartiments locataires

Étapes

1. Depuis l'une ou l'autre grille, connectez-vous au Grid Manager depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **Locataires autorisés**, déterminez si la connexion est utilisée par des locataires.
5. Si des locataires sont répertoriés, demandez à tous les locataires de "[désactiver la répllication inter-grilles](#)" le faire pour tous leurs compartiments sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grilles** si des compartiments locataires ont la répllication inter-grilles activée. Chaque compte locataire doit désactiver la répllication inter-grilles pour ses compartiments sur les deux grilles.

Supprimez l'autorisation pour chaque locataire

Une fois la répllication inter-grilles désactivée pour tous les compartiments locataires, supprimez l'autorisation

Utiliser la **fédération de grilles** de tous les locataires sur les deux grilles.

Étapes

1. Sélectionnez **Configuration > System > Grid federation**.
2. Sélectionnez le nom de la connexion pour afficher ses détails.
3. Pour chaque locataire figurant dans l'onglet **Locataires autorisés**, supprimez l'autorisation **Utiliser la connexion de fédération de grille** pour chaque locataire. Voir "[Gérer les locataires autorisés](#)".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Supprimer la connexion

Étapes

1. Lorsque aucun locataire sur l'une ou l'autre grille n'utilise la connexion, sélectionnez **Supprimer**.
2. Vérifiez le message de confirmation, puis sélectionnez **Supprimer**.
 - Si la connexion peut être supprimée, un message de confirmation s'affiche. La connexion de fédération de grilles est désormais supprimée des deux grilles.
 - Si la connexion ne peut pas être supprimée (par exemple, si elle est toujours utilisée ou en cas d'erreur de connexion), un message d'erreur s'affiche. Vous pouvez effectuer l'une des actions suivantes :
 - Résolvez l'erreur (recommandé). Voir "[Dépanner les erreurs de fédération de grille](#)".
 - Supprimez la connexion de force. Voir la section suivante.

Supprimer de force une connexion de fédération de grille

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas le statut **Connected**.

La suppression forcée ne supprime la connexion que du grid local. Pour supprimer complètement la connexion, effectuez les mêmes étapes sur les deux grids.

Étapes

1. Dans la boîte de dialogue de confirmation, sélectionnez **Force remove**.

Un message de confirmation s'affiche. Cette connexion de fédération de grilles ne peut plus être utilisée. Cependant, certains compartiments locataires peuvent encore avoir la réplication inter-grilles activée et certaines copies d'objets peuvent déjà avoir été répliquées entre les grilles de la connexion.

2. Depuis l'autre grille de la connexion, connectez-vous au Grid Manager depuis le nœud d'administration principal.
3. Sélectionnez **Configuration > System > Grid federation**.
4. Sélectionnez le nom de la connexion pour afficher ses détails.
5. Sélectionnez **Supprimer** et **Oui**.
6. Sélectionnez **Force remove** pour supprimer la connexion de cette grille.

Gérer les locataires autorisés pour la fédération de grilles StorageGRID

Vous pouvez autoriser les comptes locataires S3 à utiliser une connexion de fédération de grille entre deux systèmes StorageGRID. Lorsqu'un locataire est autorisé à utiliser une connexion, des étapes spécifiques sont nécessaires pour modifier les détails du locataire ou pour retirer définitivement l'autorisation d'utiliser la connexion.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous disposez des ["Autorisation d'accès root"](#) pour la grille à laquelle vous êtes connecté.
- Vous avez ["a créé une connexion de fédération de grille"](#) entre deux grilles.
- Vous avez examiné les flux de travail pour ["clone de compte"](#) et ["réplication inter-grilles"](#).
- Comme requis, vous avez déjà configuré l'authentification unique (SSO) ou la fédération d'identité pour les deux grilles de la connexion. Voir ["Qu'est-ce qu'un clone de compte"](#).

Créer un locataire autorisé

Si vous souhaitez autoriser un compte locataire nouveau ou existant à utiliser une connexion de fédération de grille pour le clonage de compte et la réplication inter-grilles, suivez les instructions générales pour ["créer un nouveau locataire S3"](#) ou ["modifier un compte locataire"](#) et tenez compte des points suivants :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille de la connexion. La grille sur laquelle un locataire est créé est la *grille source du locataire*.
- L'état de la connexion doit être **Connected**.
- Lorsqu'un locataire est créé ou modifié pour activer l'autorisation **Utiliser la connexion de fédération de grilles**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille sur laquelle le locataire est répliqué est la *grille de destination* du locataire.
- Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations. Vous pouvez éventuellement utiliser le champ **Description** pour vous aider à identifier lequel est le locataire source et lequel est le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 apparaîtra également pour le locataire répliqué sur la grille 2 : « Ce locataire a été créé sur la grille 1. »
- Pour des raisons de sécurité, le mot de passe de l'utilisateur root local n'est pas copié sur la grille de destination.



Avant qu'un utilisateur root local puisse se connecter au locataire répliqué sur la grille de destination, un administrateur de grille pour cette grille doit ["modifier le mot de passe de l'utilisateur root local"](#).

- Une fois le locataire nouveau ou modifié disponible sur les deux grilles, les utilisateurs locataires peuvent effectuer les opérations suivantes :
 - À partir de la grille source du locataire, créez des groupes et des utilisateurs locaux, qui sont automatiquement clonés dans la grille de destination du locataire. Voir ["Cloner les groupes de locataires et les utilisateurs"](#).
 - Créez de nouvelles clés d'accès S3, qui peuvent être clonées en option sur la grille de destination du locataire. Voir ["Cloner les clés d'accès S3 à l'aide de l'API"](#).
 - Créez des compartiments identiques sur les deux grilles de la connexion et activez la réplication inter-grilles dans un sens ou dans les deux sens. Voir ["Gérer la réplication inter-grilles"](#).

Afficher un locataire autorisé

Vous pouvez consulter les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **Tenants**.
2. Depuis la page Locataires, sélectionnez le nom du locataire pour afficher la page de détails du locataire.

Si cette grille est la grille source du locataire (c'est-à-dire si le locataire a été créé sur cette grille), une bannière s'affiche pour vous rappeler que le locataire a été cloné sur une autre grille. Si vous modifiez ou supprimez ce locataire, vos modifications ne seront pas synchronisées avec l'autre grille.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	Connected	10.96.106.230	Check for errors

3. Vous pouvez également sélectionner l'onglet **Fédération de grilles** pour "[surveiller la connexion de la fédération du grid](#)".

Modifier un locataire autorisé

Si vous devez modifier un locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille**, suivez les instructions générales "[modification d'un compte locataire](#)" et tenez compte des points suivants :

- Si un locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vous pouvez modifier les informations du locataire depuis l'une ou l'autre grille de la connexion. Cependant, toute modification que vous effectuez ne sera pas copiée sur l'autre grille. Si vous souhaitez que les informations du locataire restent synchronisées entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.

- Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une connexion de fédération de grille différente lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

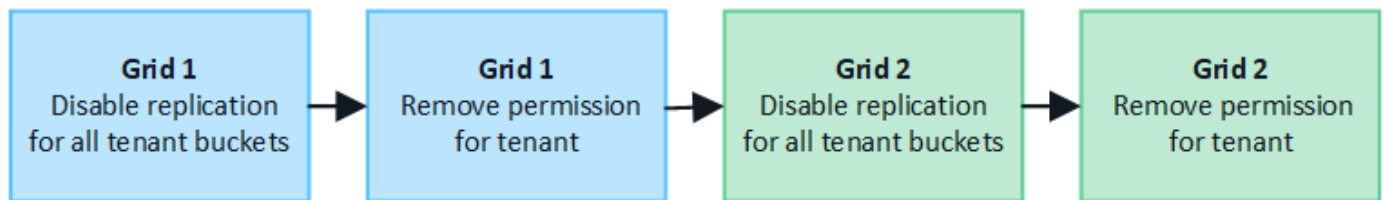
Si vous devez supprimer un locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille**, suivez les instructions générales "[suppression d'un compte locataire](#)" et tenez compte des points suivants :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer tous les compartiments pour le compte sur la grille source.
- Avant de pouvoir supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les compartiments du compte sur la grille de destination.
- Si vous supprimez le locataire d'origine ou le locataire cloné, le compte ne pourra plus être utilisé pour la réplication inter-grille.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes, utilisateurs ou clés de locataire clonés vers la grille de destination resteront inchangés. Vous pouvez soit supprimer le locataire cloné, soit lui permettre de gérer ses propres groupes, utilisateurs, clés d'accès et compartiments.
- Si vous supprimez le locataire cloné sur la grille de destination, des erreurs de clonage se produiront si de nouveaux groupes ou utilisateurs sont ajoutés au locataire d'origine.

Pour éviter ces erreurs, supprimez l'autorisation du locataire d'utiliser la connexion de fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation d'utiliser la connexion à la fédération de grille

Pour empêcher un locataire d'utiliser une connexion de fédération de grille, vous devez supprimer l'autorisation **Utiliser une connexion de fédération de grille**.



Avant de retirer à un locataire l'autorisation d'utiliser une connexion de fédération de grille, notez ce qui suit :

- Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments du locataire. Le compte du locataire doit d'abord désactiver la réplication inter-grille pour tous ses compartiments.
- La suppression de l'autorisation « Utiliser la connexion de fédération de grilles » ne supprime pas les éléments déjà répliqués entre les grilles. Par exemple, les utilisateurs, groupes et objets du locataire présents sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est retirée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Si vous souhaitez réactiver cette autorisation avec la même connexion de fédération de grille, supprimez d'abord ce locataire sur la grille de destination ; sinon, la réactivation de cette autorisation entraînera une erreur.



La réactivation de l'autorisation « Utiliser la connexion de fédération de grilles » définit la grille locale comme grille source et déclenche le clonage vers la grille distante spécifiée par la connexion de fédération de grilles sélectionnée. Si le compte du locataire existe déjà sur la grille distante, le clonage entraînera une erreur de conflit.

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#) pour les deux grilles.

Désactiver la réplication pour les compartiments locataires

Dans un premier temps, désactivez la réplication inter-grilles pour tous les compartiments locataires.

Étapes

1. Depuis l'une ou l'autre grille, connectez-vous au Grid Manager depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **Locataires autorisés**, déterminez si le locataire utilise la connexion.
5. Si le locataire est répertorié, demandez-lui de ["désactiver la réplication inter-grilles"](#) le faire pour tous ses compartiments sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grilles** si la réplication inter-grilles est activée pour au moins un compartiment locataire. Le locataire doit désactiver la réplication inter-grilles pour ses compartiments sur les deux grilles.

Supprimer l'autorisation du locataire

Une fois la réplication inter-grilles désactivée pour les compartiments de locataire, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération de grilles.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Supprimez l'autorisation depuis la page de fédération Grid ou la page des locataires.

page de fédération de grille

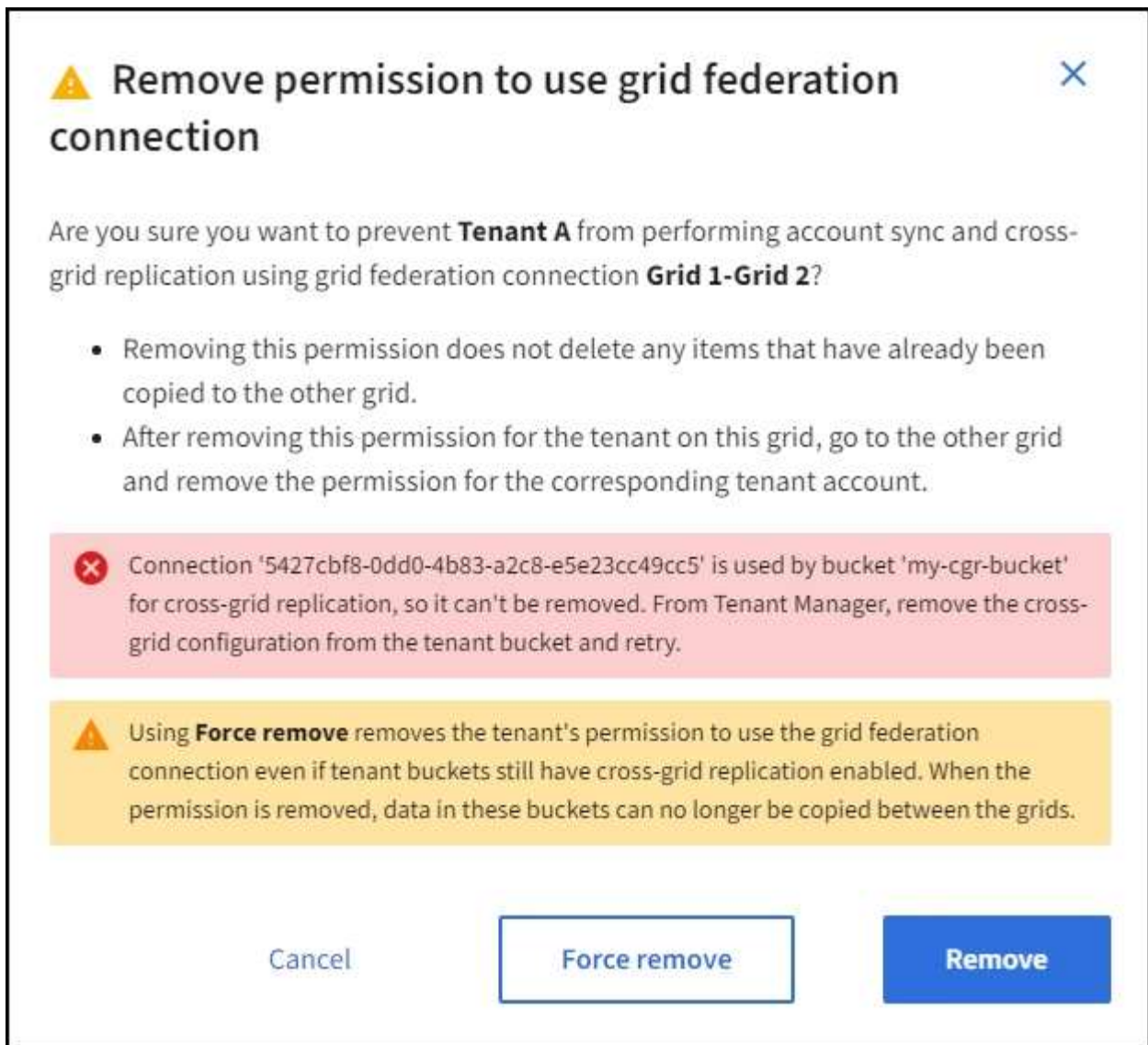
- a. Sélectionnez **Configuration > System > Grid federation**.
- b. Sélectionnez le nom de la connexion pour afficher sa page de détails.
- c. Dans l'onglet **Locataires autorisés**, sélectionnez le bouton radio correspondant au locataire.
- d. Sélectionnez **Supprimer l'autorisation**.

Page des locataires

- a. Sélectionnez **Tenants**.
- b. Sélectionnez le nom du locataire pour afficher la page de détails.
- c. Dans l'onglet **Fédération de grilles**, sélectionnez le bouton radio pour la connexion.
- d. Sélectionnez **Supprimer l'autorisation**.

3. Examinez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

- Si l'autorisation peut être supprimée, vous êtes redirigé vers la page de détails et un message de confirmation s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.
- Si un ou plusieurs compartiments locataires ont encore la réplication inter-grille activée, une erreur s'affiche.



Vous pouvez faire l'une ou l'autre des choses suivantes :

- (Recommandé.) Connectez-vous au Tenant Manager et désactivez la réplication pour chaque compartiment du locataire. Voir "[Gérer la réplication inter-grilles](#)". Ensuite, répétez les étapes pour supprimer l'autorisation **Use grid connection**.
- Supprimez l'autorisation de force. Voir la section suivante.

4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation du même locataire sur l'autre grille.

Supprimer l'autorisation de force

Si nécessaire, vous pouvez forcer la suppression de l'autorisation d'un locataire à utiliser une connexion de fédération de grille, même si les compartiments du locataire ont la réplication inter-grille activée.

Avant de retirer de force l'autorisation d'un locataire, veuillez prendre en compte les considérations générales [suppression de l'autorisation](#) ainsi que les considérations supplémentaires suivantes :

- Si vous supprimez de force l'autorisation « Utiliser la connexion de fédération de grilles », les objets en attente de réplication vers l'autre grille (ingérés mais pas encore répliqués) continueront d'être répliqués. Pour empêcher ces objets en cours de traitement d'atteindre le compartiment de destination, vous devez

également supprimer l'autorisation du locataire sur l'autre grille.

- Les objets ingérés dans le compartiment source après la suppression de l'autorisation **Utiliser la connexion de fédération de grille** ne seront jamais répliqués dans le compartiment de destination.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration > System > Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher sa page de détails.
4. Dans l'onglet **Locataires autorisés**, sélectionnez le bouton radio correspondant au locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Examinez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Force remove**.

Un message de confirmation s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.

7. Si nécessaire, accédez à l'autre grille et répétez ces étapes pour supprimer de force l'autorisation du même compte client sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours de traitement d'atteindre le compartiment de destination.

Dépanner les erreurs de fédération de grille dans StorageGRID

Vous pourriez avoir besoin de résoudre des alertes et des erreurs liées aux connexions de fédération de grilles, au clonage de comptes et à la réplication inter-grilles.

Alertes et erreurs de connexion à la fédération de grilles

Vous pourriez recevoir des alertes ou rencontrer des erreurs concernant vos connexions de fédération de grille.

Après avoir effectué des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion redevient **Connecté**. Pour obtenir des instructions, consultez ["Gérer les connexions de fédération de grille"](#).

Alerte d'échec de connexion à la fédération de grille

Problème

L'alerte **Échec de la connexion à la fédération du grid** a été déclenchée.

Détails

Cette alerte indique que la connexion de fédération de grilles entre les grilles ne fonctionne pas.

Actions recommandées

1. Vérifiez les paramètres de la page Fédération de grilles pour les deux grilles. Assurez-vous que toutes les valeurs sont correctes. Voir ["Gérer les connexions de fédération de grille"](#).
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a aucune alerte concernant l'expiration des certificats de fédération de grille et que les détails de chaque certificat sont valides. Consultez les instructions pour la rotation des certificats de connexion dans ["Gérer les connexions de fédération de grille"](#).
3. Vérifiez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez les alertes susceptibles d'affecter ces nœuds et réessayez.

4. Si vous avez fourni un domaine complet (FQDN) pour la grille locale ou distante, vérifiez que le serveur DNS est en ligne et disponible. Voir ["Qu'est-ce que la fédération de grilles ?"](#) pour les exigences en matière de réseau, d'adresse IP et de DNS.

Alerte d'expiration du certificat de fédération de grille

Problème

L'alerte **Expiration du certificat de fédération de grille** a été déclenchée.

Détails

Cette alerte indique qu'un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.

Actions recommandées

Consultez les instructions pour la rotation des certificats de connexion dans ["Gérer les connexions de fédération de grille"](#).

Erreur lors de la modification d'une connexion de fédération de grille

Problème

Lors de la modification d'une connexion de fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : « Échec de la création d'un fichier de configuration candidat sur un ou plusieurs nœuds. »

Détails

Lorsque vous modifiez une connexion de fédération de grilles, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Un message d'avertissement s'affiche si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, par exemple si un nœud d'administration est hors ligne.

Actions recommandées

1. Dans la grille que vous utilisez pour modifier la connexion, sélectionnez **Nœuds**.
2. Vérifiez que tous les nœuds d'administration de cette grille sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et essayez de modifier à nouveau la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte locataire cloné. Le message d'erreur sur la page de connexion du Tenant Manager est « Vos identifiants pour ce compte étaient invalides. Veuillez réessayer. »

Détails

Pour des raisons de sécurité, lorsque vous clonez un compte client de la grille source du client vers la grille de destination du client, le mot de passe que vous définissez pour l'utilisateur racine local du client n'est pas cloné. De même, lorsqu'un client crée des utilisateurs locaux sur sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés vers la grille de destination.

Actions recommandées

Avant que l'utilisateur racine puisse se connecter à la grille de destination du locataire, un administrateur de grille doit d'abord ["modifier le mot de passe de l'utilisateur root local"](#) sur la grille de destination.

Avant qu'un utilisateur local cloné puisse se connecter à la grille de destination du locataire, l'utilisateur root du locataire cloné doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, consultez "[Gérer les utilisateurs](#)" dans les instructions d'utilisation du Tenant Manager.

Locataire créé sans clone

Problème

Vous voyez le message « Locataire créé sans clone » après avoir créé un nouveau locataire avec l'autorisation **Utiliser la connexion de fédération de grille**.

Détails

Ce problème peut survenir si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner l'affichage d'une connexion défaillante comme **Connected**.

Actions recommandées

1. Examinez la raison indiquée dans le message d'erreur et résolvez tout problème de réseau ou autre pouvant empêcher la connexion de fonctionner. Voir [Alertes et erreurs de connexion à la fédération de grille](#).
2. Suivez les instructions pour tester une connexion de fédération de grille dans "[Gérer les connexions de fédération de grille](#)" afin de confirmer que le problème a été résolu.
3. Depuis la grille source du locataire, sélectionnez **Tenants**.
4. Localisez le compte locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clonage du compte**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions

✖

Tenant account could not be cloned to the other grid.

Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Si l'erreur a été résolue, le compte du locataire sera maintenant cloné sur l'autre grille.

Alertes et erreurs de réplication inter-grilles

Dernière erreur affichée pour la connexion ou le tenant

Problème

Lorsque "visualisation d'une connexion de fédération de grille" (ou lorsque "gérer les locataires autorisés" pour une connexion), vous constatez une erreur dans la colonne **Dernière erreur** sur la page des détails de la connexion. Par exemple :

Grid 1 - Grid 2

Local hostname (this grid):10.115.96.170

Port:23000

Remote hostname (other grid):10.115.96.175

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	2025-03-13 15:54:59 PDT Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled. (logID 13371653720226059496) Check for errors

Détails

Pour chaque connexion de fédération de grilles, la colonne **Dernière erreur** affiche la dernière erreur survenue, le cas échéant, lors de la réplication des données d'un locataire vers l'autre grille. Cette colonne n'affiche que la dernière erreur de réplication inter-grilles ; les erreurs précédentes qui auraient pu se produire ne sont pas affichées. Une erreur dans cette colonne peut survenir pour l'une des raisons suivantes :

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un compte différent.
- Le versionnage du bucket de destination est suspendu.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.
- L'objet source possède des paramètres de verrouillage d'objet S3 qui ne sont pas conformes aux paramètres de rétention au niveau du locataire de la grille de destination.
- L'objet source possède des paramètres de verrouillage d'objet S3 et le verrouillage d'objet S3 est désactivé sur le compartiment de destination.

Actions recommandées

Si un message d'erreur apparaît dans la colonne **Dernière erreur**, suivez ces étapes :

1. Veuillez vérifier le texte du message.
2. Effectuez les actions recommandées. Par exemple, si le versionnage a été suspendu sur le compartiment de destination pour la réplication inter-grilles, réactivez le versionnage pour ce compartiment.
3. Sélectionnez la connexion ou le compte locataire dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.

6. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage du message avant d'ingérer un nouvel objet.



Une fois l'erreur résolue, une nouvelle **Dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui présente également une erreur.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, consultez ["Identifier et réessayer les opérations de réplication ayant échoué"](#).

Alerte de défaillance permanente de la réplication inter-grid

Problème

L'alerte **Échec permanent de la réplication inter-grilles** a été déclenchée.

Détails

Cette alerte indique que la réplication des objets locataires entre les compartiments de deux grilles est impossible pour une raison nécessitant l'intervention de l'utilisateur. Cette alerte est généralement due à une modification apportée au compartiment source ou au compartiment de destination.

Actions recommandées

1. Connectez-vous à la grille où l'alerte a été déclenchée.
2. Accédez à **Configuration > Système > Fédération de grilles**, et repérez le nom de la connexion indiqué dans l'alerte.
3. Dans l'onglet Locataires autorisés, consultez la colonne **Dernière erreur** pour déterminer quels comptes locataires présentent des erreurs.
4. Pour en savoir plus sur cette défaillance, consultez les instructions dans ["Surveiller les connexions de fédération de la grille"](#) pour examiner les indicateurs de réplication inter-grilles.
5. Pour chaque compte locataire concerné :
 - a. Consultez les instructions dans ["Surveiller l'activité des locataires"](#) pour confirmer que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grilles.
 - b. Au besoin, augmentez le quota du locataire sur la grille de destination pour permettre l'enregistrement de nouveaux objets.
6. Pour chaque locataire concerné, connectez-vous à Tenant Manager sur les deux grilles afin de pouvoir comparer la liste des compartiments.
7. Pour chaque compartiment pour lequel la réplication inter-grilles est activée, confirmez les points suivants :
 - Il existe un compartiment correspondant pour le même locataire sur l'autre grille (vous devez utiliser le nom exact).
 - Les deux compartiments ont le versionnage des objets activé (le versionnage ne peut pas être suspendu sur aucune des deux grilles).
 - Aucun des deux compartiments n'est dans l'état **Suppression d'objets : lecture seule**.
8. Pour confirmer que le problème a été résolu, consultez les instructions dans ["Surveiller les connexions de fédération de la grille"](#) pour examiner les indicateurs de réplication inter-grilles, ou effectuez les étapes suivantes :

- a. Revenez à la page Grid federation.
- b. Sélectionnez le locataire concerné, puis sélectionnez **Effacer l'erreur** dans la colonne **Dernière erreur**.
- c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
- d. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage du message avant d'ingérer un nouvel objet.



Il peut s'écouler jusqu'à une journée avant que l'alerte ne disparaisse après sa résolution.

- a. Accédez à "[Identifier et réessayer les opérations de réplication ayant échoué](#)" pour identifier les objets ou les marqueurs de suppression qui n'ont pas pu être répliqués sur l'autre grille et pour réessayer la réplication si nécessaire.

Alerte de ressource de réplication inter-grilles indisponible

Problème

L'alerte **Ressource de réplication inter-grilles indisponible** a été déclenchée.

Détails

Cette alerte indique que des requêtes de réplication inter-réseaux sont en attente car une ressource est indisponible. Par exemple, il peut s'agir d'une erreur réseau.

Actions recommandées

1. Surveillez l'alerte pour voir si le problème se résout de lui-même.
2. Si le problème persiste, déterminez si l'une des grilles présente une alerte **Échec de la connexion à la fédération de grilles** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte pourrait être résolue lorsque vous aurez résolu ces alertes.
3. Pour en savoir plus sur cette défaillance, consultez les instructions dans "[Surveiller les connexions de fédération de la grille](#)" pour examiner les indicateurs de réplication inter-grilles.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grilles reprendra son cours normal une fois le problème résolu.

Identifier et réessayer les opérations de réplication StorageGRID ayant échoué

Après avoir résolu l'alerte « Échec permanent de la réplication inter-grilles », vous devez déterminer si des objets ou des marqueurs de suppression n'ont pas pu être répliqués vers l'autre grille. Vous pouvez ensuite réingérer ces objets ou utiliser l'API de gestion Grid Management pour réessayer la réplication.

L'alerte **Échec permanent de la réplication inter-grilles** indique que les objets locataires ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison nécessitant l'intervention de l'utilisateur. Cette alerte est généralement causée par une modification du compartiment source ou du compartiment de destination. Pour plus de détails, consultez "[Dépanner les erreurs de fédération de grille](#)".

Déterminez si des objets ont échoué à être répliqués

Pour déterminer si des objets ou des marqueurs de suppression n'ont pas été répliqués sur l'autre grille, vous pouvez rechercher dans le journal des audits les messages "[CGRR \(Demande de réplication inter-grilles\)](#)". Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet multipart ou un marqueur de suppression vers le compartiment de destination.

Vous pouvez utiliser le "[outil audit-explain](#)" pour traduire les résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez des droits d'accès root.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
 - c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
 - d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

2. Recherchez les messages CGRR dans le journal des audits `audit.log` et utilisez l'outil `audit-explain` pour formater les résultats.

Par exemple, cette commande recherche tous les messages CGRR des 30 dernières minutes et utilise l'outil `audit-explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

Les résultats de la commande ressembleront à cet exemple, qui contient les entrées de six messages CGRR. Dans l'exemple, toutes les requêtes de réplication inter-grilles ont renvoyé une erreur générale, car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent des opérations de « replicate object », et les trois dernières erreurs concernent des opérations de « replicate delete marker ».

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error

```

Chaque entrée contient les informations suivantes :

Champ	Description
Demande de réplication inter-grilles CGRR	Le nom de la demande
locataire	L'identifiant du compte du locataire
connexion	L'identifiant de la connexion de la fédération de grille
opération	Le type d'opération de réplication qui était en cours de tentative : • répliquer l'objet • répliquer le marqueur de suppression • répliquer un objet multipart
bucket	Le nom du compartiment
objet	Le nom de l'objet
version	L'identifiant de version de l'objet

Champ	Description
erreur	Type d'erreur. En cas d'échec de la réplication inter-grilles, l'erreur est « Erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste des objets et des marqueurs de suppression qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de deux manières :

- Réingérez chaque objet dans le compartiment source.
- Utilisez l'API privée de gestion de la grille, comme décrit.

Étapes

1. En haut du Grid Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
2. Sélectionnez **Accéder à la documentation de l'API privée**.



Les points de terminaison de l'API StorageGRID marqués « Privé » sont susceptibles d'être modifiés sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

3. Dans la section **cross-grid-replication-advanced**, sélectionnez l'endpoint suivant :

```
POST /private/cross-grid-replication-retry-failed
```

4. Sélectionnez **Try it out**.
5. Dans la zone de texte **corps**, remplacez l'exemple d'entrée pour **versionID** par un ID de version du journal des audits qui correspond à une requête de réplication inter-grille ayant échoué.

Veillez à conserver les guillemets doubles autour de la chaîne de caractères.

6. Sélectionnez **Exécuter**.
7. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que l'objet ou le marqueur de suppression a été marqué comme en attente de réplication inter-grille vers l'autre grille.



« En attente » signifie que la demande de réplication inter-grille a été ajoutée à la file d'attente interne pour traitement.

Surveillez les tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles aboutissent.



La réplication d'un objet ou d'un marqueur de suppression vers l'autre grille peut prendre plusieurs heures ou plus.

Vous pouvez surveiller les opérations de nouvelle tentative de deux manières :

- Utilisez une requête S3 "[HeadObject](#)" ou "[GetObject](#)". La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grid	État de la réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué de manière permanente. Un utilisateur doit résoudre l'erreur.
Destination	REPLICA : L'objet a été répliqué à partir de la grille source.

- Utilisez l'API privée de gestion de la grille, comme décrit.

Étapes

1. Dans la section **cross-grid-replication-advanced** de la documentation de l'API privée, sélectionnez le point de terminaison suivant :

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Sélectionnez **Try it out**.
3. Dans la section Paramètres, saisissez l'identifiant de version que vous avez utilisé dans la `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Vérifiez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de la réplication, qui sera l'un des suivants :
 - **EN ATTENTE** : L'objet n'a pas encore été répliqué.
 - **TERMINÉ** : La réplication a réussi.
 - **ÉCHEC** : La réplication a échoué de manière permanente. Un utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité dans StorageGRID

Vous pouvez configurer différents paramètres de sécurité depuis le Grid Manager pour contribuer à la sécurité de votre système StorageGRID.

Gérer le chiffrement

StorageGRID propose plusieurs options de chiffrement des données. Il vous appartient "[examiner les méthodes de chiffrement disponibles](#)" de déterminer celles qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Vous pouvez "[configurer et gérer les certificats du serveur](#)" utiliser pour les connexions HTTP ou les certificats clients utilisés pour authentifier l'identité d'un client ou d'un utilisateur auprès du serveur.

Configurer les serveurs de gestion des clés

L'utilisation d'une "[serveur de gestion des clés](#)" vous permet de protéger les données StorageGRID même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif à moins que le nœud puisse communiquer avec le KMS.



Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Chiffrement de nœud** pour chaque appareil lors de l'installation, avant que l'appareil ne soit ajouté à la grille.

Gérer les paramètres du proxy

Si vous utilisez les services de la plateforme S3 ou des Cloud Storage Pools, vous pouvez configurer une "[serveur proxy de stockage](#)" entre les nœuds de stockage et les points de terminaison S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un "[serveur proxy d'administration](#)" entre les nœuds d'administration et le support technique.

Contrôlez les pare-feu

Pour renforcer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou fermant des ports spécifiques au "[pare-feu externe](#)". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "[pare-feu interne](#)". Vous pouvez bloquer l'accès sur tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Passez en revue les méthodes de chiffrement de StorageGRID

StorageGRID propose plusieurs options de chiffrement des données. Vous devez examiner les méthodes disponibles afin de déterminer celles qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un résumé général des méthodes de chiffrement disponibles dans StorageGRID.

Option de chiffrement	Comment ça marche	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous " configurer un serveur de gestion des clés " pour le site StorageGRID et " activer le chiffrement 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 (DEK) sur chaque volume.	Les nœuds d'appliance dont la fonction Node Encryption est activée lors de l'installation. Toutes les données sur l'appliance sont protégées contre toute perte physique ou tout retrait du centre de données. Remarque : La gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.

Option de chiffrement	Comment ça marche	S'applique à
Page de chiffrement du disque dans l'installateur de l'appliance StorageGRID	Si l'appliance contient des disques prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de disque lors de l'installation. Lorsque vous définissez une phrase secrète de disque, il est impossible pour quiconque de récupérer des données valides à partir de disques retirés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, allez dans Configure Hardware > Drive Encryption pour définir une phrase secrète de disque qui s'appliquera à tous les disques à chiffrement automatique gérés par StorageGRID dans un nœud.	Les appareils équipés de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Le chiffrement des disques ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'un système de stockage avec des disques à chiffrement automatique et des contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonction de sécurité des disques est activée pour votre StorageGRID appliance, vous pouvez utiliser " SANtricity System Manager " pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données des disques sécurisés.	Les appliances de stockage équipées de disques à chiffrement intégral (FDE) ou de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Ne peut pas être utilisé avec certains appliances de stockage ni avec aucune appliance de services.
Chiffrement des objets stockés	Vous activez l'option " Chiffrement des objets stockés " dans le Gestionnaire de grille. Une fois activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du compartiment ou au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées.

Option de chiffrement	Comment ça marche	S'applique à
chiffrement du compartiment S3	Vous envoyez une requête PutBucketEncryption pour activer le chiffrement du compartiment. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de leur ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets existants du compartiment ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur des objets S3 (SSE)	Vous envoyez une requête S3 pour stocker un objet et incluez l x-amz-server-side-encryption en-tête de la requête.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le chiffrement côté serveur"
Chiffrement côté serveur S3 des objets avec des clés fournies par le client (SSE-C)	Vous envoyez une requête S3 pour stocker un objet et incluez trois en-têtes de requête. - x-amz-server-side-encryption-customer-algorithm - x-amz-server-side-encryption-customer-key - x-amz-server-side-encryption-customer-key-MD5	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utilisez le chiffrement côté serveur"

Option de chiffrement	Comment ça marche	S'applique à
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, les métadonnées et les données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer les données et les métadonnées des objets avant leur ingestion dans StorageGRID.	Données et métadonnées de l'objet uniquement (les données de configuration système ne sont pas chiffrées). Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées. "Amazon Simple Storage Service - Guide de l'utilisateur : Protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement simultanément. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et également utiliser la fonction de sécurité des disques dans SANtricity System Manager pour « double chiffrer » les données sur les disques à chiffrement automatique des mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds de l'appliance et également utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lors de leur ingestion.

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez de contrôler le chiffrement au niveau du compartiment ou de chaque objet à la place. L'activation de plusieurs niveaux de chiffrement engendre un coût supplémentaire en termes de performances.

Informations connexes

["Découvrez les options de chiffrement certifiées FIPS"](#)

Gérer les certificats

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

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- Les certificats clients authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne chiffrent pas les données.

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

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

Certificat CA Grid par défaut

StorageGRID intègre une autorité de certification (CA) qui génère un certificat Grid CA interne lors de l'installation du système. Le certificat Grid CA est utilisé par défaut pour sécuriser le trafic interne de StorageGRID. Une autorité de certification (CA) externe peut émettre des certificats personnalisés, entièrement conformes aux politiques de sécurité informatique de votre organisation.

Utilisez le certificat de l'autorité de certification Grid pour les environnements hors production. Pour la production, utilisez des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont prises en charge, mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne remplacent pas les certificats internes ; toutefois, ce sont les certificats personnalisés qui doivent être spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent respecter les "[Recommandations de renforcement du système pour les certificats de serveur](#)".
- StorageGRID prend en charge le regroupement des certificats d'une autorité de certification dans un seul fichier (appelé ensemble de certificats d'une autorité de certification).



StorageGRID inclut également des certificats d'autorité de certification (CA) du système d'exploitation, identiques sur toutes les grilles. En environnement de production, veuillez à spécifier un certificat personnalisé signé par une autorité de certification externe, en remplacement du certificat CA du système d'exploitation.

Les différents types de certificats serveur et client sont implémentés de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID avant de configurer le système.

Certificats de sécurité d'accès

Vous pouvez accéder aux informations concernant tous les certificats StorageGRID en un seul endroit, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, sélectionnez **Configuration > Security > Certificates**.

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 accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le ["autorisation appropriée"](#).
 - **Global** : Sécurise l'accès à StorageGRID depuis les navigateurs web et les clients API externes.
 - **Autorité de certification Grid** : Sécurise le trafic interne de StorageGRID.
 - **Client** : Sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
 - **Points de terminaison de l'équilibreur de charge** : Sécurisent les connexions entre les clients S3 et l'équilibreur de charge StorageGRID.
 - **Locataires** : Sécurise les connexions aux serveurs de fédération d'identité ou depuis les points de terminaison de service de la plateforme vers les 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 supplémentaires sur le certificat.

Global

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

- [Certificat d'interface de gestion](#): Sécurise les connexions des navigateurs web clients aux interfaces de gestion StorageGRID.
- [Certificat API S3](#): Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications clientes S3 utilisent pour charger et télécharger des données d'objet.

Les informations relatives aux 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 une sécurité renforcée de la grille :
 - ["Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID"](#) Utilisé pour les connexions de Grid Manager et de Tenant Manager.
 - ["Remplacez le certificat de l'API S3"](#) utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (optionnel).
- ["Restaurez le certificat d'interface de gestion par défaut"](#).
- ["Restaurez le certificat d'API S3 par défaut"](#).
- ["Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé"](#).
- Copiez ou téléchargez le ["certificat d'interface de gestion"](#) ou ["Certificat API S3"](#).

Grid CA

Le [Certificat d'autorité de certification Grid](#) généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic interne de StorageGRID.

Les informations relatives au certificat comprennent la date d'expiration du certificat et le contenu du certificat.

Vous pouvez ["Copiez ou téléchargez le certificat Grid CA"](#), mais vous ne pouvez pas le changer.

Client

[Certificats clients](#), générés par une autorité de certification externe, sécurisent les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

Le tableau des certificats comporte une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que sa date d'expiration.

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 les autorisations d'accès à Prometheus."](#)
 - ["Téléchargez et remplacez le certificat client."](#)
 - ["Copiez ou téléchargez le certificat client."](#)
 - ["Supprimez le certificat client."](#)
- Sélectionnez **Actions** pour ["modifier"](#), ["attacher"](#) ou ["retirer"](#) un certificat client rapidement. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément via **Actions** > **Supprimer**.

points de terminaison de l'équilibreur de charge

[Certificats de point de terminaison de l'équilibreur de charge](#) sécuriser les connexions entre les clients S3 et le service Load Balancer StorageGRID sur les nœuds de passerelle et les nœuds d'administration.

Le tableau des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison configuré et indique si le certificat d'API S3 global ou un certificat personnalisé de point de terminaison d'équilibreur de charge est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.



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

Vous pouvez :

- ["Afficher un point de terminaison d'équilibrage de charge"](#), y compris les détails de son certificat.
- ["Spécifiez un certificat de point de terminaison d'équilibreur de charge pour FabricPool."](#)
- ["Utilisez le certificat d'API S3 global"](#) au lieu de générer un nouveau certificat de point de terminaison d'équilibrage de charge.

locataires

Les locataires peuvent utiliser [certificats de serveur de fédération d'identité](#) ou [certificats de point de terminaison de service de plateforme](#) pour sécuriser leurs connexions avec StorageGRID.

Le tableau des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Vous pouvez :

- ["Sélectionnez un nom de locataire pour vous connecter au Tenant Manager"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme du locataire"](#)
- ["Spécifiez un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"](#)

Autre

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

- [Certificats du pool de stockage cloud](#)
- [Certificats de notification d'alerte par e-mail](#)
- [Certificats de serveur syslog externe](#)
- [Certificats de connexion à la fédération de grille](#)
- [Certificats de fédération d'identité](#)
- [Certificats de serveur de gestion de clés \(KMS\)](#)
- [Certificats d'authentification unique](#)

Les informations indiquent le type de certificat qu'une fonction utilise ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. Sélectionner un nom de fonction ouvre un onglet du navigateur où vous pouvez consulter et modifier les détails du certificat.



Vous ne pouvez consulter et accéder aux informations des autres certificats que si vous disposez du ["autorisation appropriée"](#).

Vous pouvez :

- ["Spécifiez un certificat de Cloud Storage Pool pour S3, C2S S3 ou Azure"](#)
- ["Spécifiez un certificat pour les notifications par e-mail d'alerte"](#)
- ["Utilisez un certificat pour un serveur syslog externe"](#)
- ["Faites pivoter les certificats de connexion à la fédération de grille"](#)
- ["Afficher et modifier un certificat de fédération d'identité"](#)
- ["Téléversez les certificats serveur et client du serveur de gestion des clés \(KMS\)"](#)
- ["Spécifiez manuellement un certificat SSO pour une relation d'approbation de partie utilisatrice"](#)

Détails du certificat de sécurité

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

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs web clients et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans avertissement de sécurité. Ce certificat authentifie également les connexions à l'API de gestion de la grille et à l'API de gestion des locataires. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	Configuration > Sécurité > Certificats , sélectionnez l'onglet Global , puis sélectionnez Certificat d'interface de gestion	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	Configuration > Sécurité > Certificats , sélectionnez l'onglet Global , puis sélectionnez S3 API certificate	"Configurer les certificats de l'API S3"

Certificat d'autorité de certification Grid

Voir la [Description du certificat d'autorité de certification Default Grid](#).

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, il permet à StorageGRID d'authentifier l'accès des clients externes. • Permet aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	Configuration > Sécurité > Certificats puis sélectionnez l'onglet Client	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibrage de charge lors de la configuration d'un point de terminaison d'équilibrage de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer des données d'objets. Vous pouvez également utiliser une version personnalisée du Certificat API S3 certificat global pour authentifier les connexions au service de Load Balancer. Si le certificat global est utilisé pour authentifier les connexions au Load Balancer, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison du Load Balancer. Remarque : Le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus fréquemment utilisé lors du fonctionnement normal de StorageGRID.	Configuration > Réseau > Points de terminaison de l'équilibreur de charge	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

certificat de point de terminaison Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un StorageGRID Cloud Storage Pool à un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob storage. Un certificat différent est requis pour chaque type de fournisseur de cloud.	ILM > Pools de stockage	"Créer un pool de stockage cloud"

Certificat de notification d'alerte par courriel

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID qui est utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification (CA) du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP exige des certificats clients pour l'authentification.	Alertes > Configuration des e-mails	"Configurer 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 enregistre les événements dans StorageGRID. Remarque : Un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	Configuration > Surveillance > Serveur d'audit et de syslog	"Utilisez un serveur syslog externe"

Certificat de connexion à la fédération Grid

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et chiffrez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grilles.	Configuration > Système > Fédération de grilles	• "Créer des connexions de fédération de grille" • "Rotation des certificats de connexion"

certificat de fédération d'identité

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération d'identité, ce qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	Configuration > Contrôle d'accès > Fédération d'identité	"Utilisez la fédération d'identités"

certificat de serveur de gestion de clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion de clés externe (KMS), qui fournit des clés de chiffrement aux nœuds de l'appliance StorageGRID.	Configuration > Sécurité > Serveur de gestion des clés	"Ajouter un serveur de gestion des clés (KMS)"

certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	Tenant Manager > STOCKAGE (S3) > Points de terminaison des services de plateforme	"Créer un point de terminaison de services de plateforme" "Modifier le point de terminaison des services de plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS), et StorageGRID utilisés pour les demandes d'authentification unique (SSO).	Configuration > Contrôle d'accès > Authentification unique	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : Service d'équilibrage de charge

Dans cet exemple, StorageGRID fait office de serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléversez le même certificat sur le client.

3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge via HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et avec une signature basée sur la clé privée.
5. Le client compare la signature du serveur à celle figurant sur sa copie du certificat. Si les signatures correspondent, le client établit une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID fait office de client.

1. À l'aide d'un logiciel Key Management Server externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat serveur signé par une autorité de certification (CA), un certificat client public et la clé privée du 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 des données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond en utilisant la connexion validée.

Types de certificats serveur pris en charge dans StorageGRID

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).



Le type de chiffrement de la politique de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA nécessitent des certificats ECDSA. Voir "[Gérer les certificats de sécurité](#)". Si vous configurez une politique de sécurité personnalisée qui n'est pas compatible avec le certificat du serveur, vous pouvez "[rétablir temporairement la politique de sécurité par défaut](#)".

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez "[Sécurité pour les clients S3](#)".

Configurez les certificats d'interface de gestion dans StorageGRID

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un certificat personnalisé unique permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans rencontrer d'avertissements de sécurité. Vous pouvez également rétablir le certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

Par défaut, chaque nœud d'administration reçoit un certificat signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat d'interface de gestion personnalisé commun et la clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds

d'administration, vous devez spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au Grid Manager et au Tenant Manager. Définissez le certificat personnalisé de manière à ce qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez effectuer la configuration sur le serveur et, selon l'autorité de certification racine (CA) que vous utilisez, les utilisateurs devront peut-être également installer le certificat de l'autorité de certification Grid dans le navigateur web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.



Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration du certificat serveur pour l'interface de gestion** est déclenchée lorsque ce certificat est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration > Sécurité > Certificats** et en vérifiant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.



Si vous accédez au Gestionnaire de grille 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 possibilité de contournement si l'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous [revenez d'un certificat d'interface de gestion personnalisé au certificat du serveur par défaut](#).

Ajouter un certificat d'interface de gestion personnalisé

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

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (.key).



Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **CA bundle** : Fichier optionnel unique contenant les certificats de chaque autorité de certification (CA) intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA encodés en 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 importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans son propre onglet.

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

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

Par exemple : storagegrid_certificate.pem

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

Générer un certificat

Générez les fichiers de certificat du serveur.



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

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. Remarque : Laissez cette case cochée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

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 son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

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



Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à une journée pour que les alertes d'expiration de certificat associées disparaissent.

6. Après avoir ajouté un certificat d'interface de gestion personnalisé, la page du certificat d'interface de gestion affiche des informations détaillées sur les certificats utilisés. Vous pouvez télécharger ou copier le PEM du certificat si nécessaire.

Restaurez le certificat d'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid Manager et Tenant Manager.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat 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 ultérieures.

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

Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` fichier.

À propos de cette tâche

La bonne 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. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
 - c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
 - d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

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

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

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



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

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

Le résultat obtenu contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'invite de commandes. `$ 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 **Certificat d'interface de gestion**.

7. Configurez votre client de gestion pour qu'il utilise le certificat public que vous avez copié. Incluez les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

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

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

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

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

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

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

Si vous copiez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Configurer les certificats d'API S3 dans StorageGRID

Vous pouvez remplacer ou restaurer le certificat serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison d'équilibrage de charge. Le certificat serveur personnalisé de remplacement est spécifique à votre organisation.



Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Configurez les certificats d'API S3 et Swift"](#).

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat serveur X.509 signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat serveur personnalisé unique et la clé privée correspondante.

Un seul certificat serveur personnalisé est utilisé pour tous les nœuds de stockage, donc vous devez spécifier le certificat comme un certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration du serveur terminée, vous devrez peut-être également installer le certificat Grid CA

dans le client API S3 que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.



Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte « Expiration du certificat serveur global pour l'API S3 » est déclenchée lorsque le certificat racine du serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **Configuration > Sécurité > Certificats** et en consultant la date d'expiration du certificat de l'API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat d'API S3 personnalisé.

Ajouter un certificat d'API S3 personnalisé

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (.key).



Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **Ensemble d'autorités de certification (CA bundle)** : Fichier optionnel unique contenant les certificats de chaque autorité de certification intermédiaire. Le fichier doit contenir chaque fichier de certificat d'autorité de certification au format PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM de chaque certificat d'API S3 personnalisé que vous avez chargé. Si vous avez chargé un bundle CA optionnel, chaque certificat s'affiche dans son propre onglet.

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

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

Par exemple : storagegrid_certificate.pem

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

Générer un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. Remarque : Laissez cette case cochée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**.

Le certificat serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

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



Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à une journée pour que les alertes d'expiration de certificat associées disparaissent.

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

7. Après avoir ajouté un certificat d'API S3 personnalisé, la page du certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé actuellement utilisé. Vous pouvez télécharger ou copier le PEM du certificat selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez rétablir l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat d'API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez **Utiliser le certificat par défaut**.

Lorsque vous restaurez la version par défaut du certificat d'API S3 global, les fichiers de certificat serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'API S3 par défaut sera utilisé pour les nouvelles connexions client S3 ultérieures aux Storage Nodes.

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

Si vous disposez des droits d'accès root et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles avec le certificat API S3 par défaut s'affiche. Accédez à ["Configurer les points de terminaison de l'équilibreur de charge"](#) pour modifier ou supprimer les points de terminaison concernés.

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

Téléchargez ou copiez le certificat de l'API S3

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

Étapes

1. Sélectionnez **Configuration > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez l'onglet **Serveur** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

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

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

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

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

Si vous copiez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

Informations connexes

- ["Utilisez l'API REST S3"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

Copiez le certificat d'autorité de certification (CA) StorageGRID Grid

StorageGRID utilise une autorité de certification interne (CA) pour sécuriser le trafic interne. Ce certificat ne change pas si vous importez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

À propos de cette tâche

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

Étapes

1. Sélectionnez **Configuration > Security > Certificates** puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat .pem.

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

Par exemple : `storagegrid_certificate.pem`

Copier le 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`

Configurer les certificats StorageGRID pour FabricPool

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

Avant de commencer

- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

Lors de la création d'un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat serveur auto-signé ou importer un certificat signé par une autorité de certification (CA) reconnue. Dans les environnements de production, vous devez utiliser un certificat signé par une CA reconnue. Les certificats signés par une CA peuvent être renouvelés sans interruption de service. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type homme du milieu.

Les étapes suivantes fournissent des instructions générales pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures détaillées, consultez ["Configurer StorageGRID pour FabricPool"](#).

Étapes

1. Vous pouvez éventuellement configurer un groupe à haute disponibilité (HA) pour que FabricPool puisse l'utiliser.
2. Créez un point de terminaison d'équilibrage de charge S3 pour que FabricPool puisse l'utiliser.

Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et, éventuellement, le bundle d'autorité de certification.

3. Intégrez StorageGRID en tant que niveau cloud dans ONTAP.

Veuillez indiquer le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat d'autorité de certification que vous avez importé. Ensuite, fournissez le certificat d'autorité de certification.



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

Configurez les certificats clients dans StorageGRID

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID, offrant ainsi un moyen sécurisé pour les outils externes de surveiller StorageGRID.

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

Voir ["Gérer les certificats de sécurité"](#) et ["Configurer les certificats de serveur personnalisés"](#).



Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat serveur est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration > Sécurité > Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.



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

Avant de commencer

- Vous disposez des droits d'accès root.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Pour configurer un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
 - Si vous avez configuré le certificat de l'interface de gestion StorageGRID, vous disposez de l'autorité de certification, du certificat client et de la clé privée 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 sauvegardée ou enregistrée lors de sa création. Si vous ne possédez pas la clé privée d'origine, vous devez en créer une nouvelle.

- Pour modifier un certificat client :
 - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
 - Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (le cas échéant) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- [Le certificat d'interface de gestion est déjà configuré](#)
- [Certificat client délivré par CA](#)
- [Certificat généré par Grid Manager](#)

Le certificat d'interface de gestion est 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 **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre les certificats**, téléversez le certificat de l'interface de gestion.
 - a. Sélectionnez **Téléverser le certificat**.
 - b. Sélectionnez **Parcourir** et sélectionnez le fichier de certificat de l'interface de gestion (.pem).
 - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Le nouveau certificat apparaît dans l'onglet Client.

7. [Configurer un outil de surveillance externe](#), comme Grafana.

Certificat client délivré par CA

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client et une clé privée émis par une autorité de certification (CA).

Étapes

1. Effectuez les étapes pour ["configurer un certificat d'interface de gestion"](#).
2. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez

l'onglet **Client**.

3. Sélectionnez **Add**.
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continue**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle d'autorité de certification :
 - a. Sélectionnez **Téléverser le certificat**.
 - b. Sélectionnez **Parcourir** et sélectionnez les fichiers du certificat client, de la clé privée et du bundle CA (.pem).
 - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Les nouveaux certificats apparaissent dans l'onglet Client.

8. [Configurer un outil de surveillance externe](#), comme Grafana.

Certificat généré par Grid Manager

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Configuration > Sécurité > Certificats**, puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
 - **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
 - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
 - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

Ces extensions définissent la finalité de la clé contenue dans le certificat.



Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **Générer**.

9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.



Vous ne pourrez plus consulter la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée dans un fichier.

Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Grid Manager, sélectionnez **Configuration > Security > Certificates** puis sélectionnez l'onglet **Global**.

12. Sélectionnez **certificat d'interface de gestion**.

13. Sélectionnez **Utiliser un certificat personnalisé**.

14. Téléversez les fichiers `certificate.pem` et `private_key.pem` de l'[Détails du certificat client](#) étape. Il n'est pas nécessaire de téléverser le bundle CA.

- Sélectionnez **Téléverser le certificat** puis **Continuer**.
- Téléchargez chaque fichier de certificat (`.pem`).
- Sélectionnez **Enregistrer** pour enregistrer le certificat dans le Grid Manager.

Le nouveau certificat apparaît sur la page des certificats de l'interface de gestion.

15. [Configurer un outil de surveillance externe](#), comme Grafana.

Configurer un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tel que Grafana.

- Nom** : Saisissez un nom pour la connexion.

StorageGRID n'a pas besoin de ces informations, mais vous devez fournir un nom pour tester la connexion.

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

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

- c. Activez l'**authentification client TLS** et **Avec certificat d'autorité de certification (CA)**.

- d. Sous Détails d'authentification TLS/SSL, copiez et collez : +

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

- e. **ServerName** : Entrez le nom de domaine du nœud d'administration.

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

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés depuis StorageGRID ou un fichier local.

Vous pouvez désormais accéder aux métriques Prometheus de StorageGRID avec votre outil de surveillance externe.

Pour plus d'informations sur les indicateurs, consultez le "[Instructions pour la surveillance StorageGRID](#)".

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour en changer le nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration > Security > Certificates** puis sélectionnez l'onglet **Client**.

Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis **Modifier le nom et les permissions**
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le 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 le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Téléverser 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 PEM du certificat.

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

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
- c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Le certificat mis à jour s'affiche dans l'onglet Client.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

- a. Sélectionnez **Générer un certificat**.
- b. Spécifiez les informations du certificat :

- **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
- **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
- **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

Ces extensions définissent la finalité de la clé contenue dans le certificat.



Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

- c. Sélectionnez **Générer**.
- d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.



Vous ne pourrez plus consulter la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

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

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

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée dans un fichier.

Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Le nouveau certificat apparaît dans l'onglet Client.

Télécharger ou copier les certificats clients

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration > Security > Certificates** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

- a. Sélectionnez **Télécharger le certificat**.
- b. Spécifiez le nom du fichier de certificat et son 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 clients

Si vous n'avez plus besoin d'un certificat client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **Configuration > Security > Certificates** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer** puis confirmez.



Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet Client, puis sélectionnez **Actions > Delete**.

Après la suppression d'un certificat, les clients qui utilisaient ce certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les paramètres de sécurité

Gérez la politique TLS et SSH dans StorageGRID

La politique TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées avec les services internes de StorageGRID.

La politique de sécurité détermine la façon dont TLS et SSH chiffrent les données en transit. En général, utilisez la politique Modern compatibility (par défaut), sauf si votre système doit être conforme aux Common Criteria ou si vous devez utiliser d'autres algorithmes de chiffrement.



Certains services StorageGRID n'ont pas été mis à jour pour utiliser les algorithmes de chiffrement définis dans ces politiques.

Avant de commencer

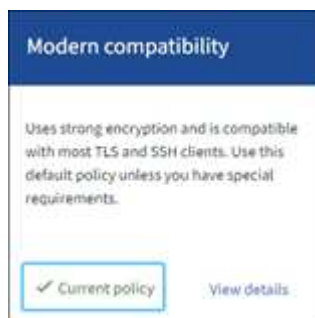
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".

Sélectionnez une politique de sécurité

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.

L'onglet **Stratégies TLS et SSH** affiche les stratégies disponibles. La stratégie actuellement active est indiquée par une coche verte sur la vignette de la stratégie.



2. Consultez les onglets pour en savoir plus sur les stratégies disponibles.

Compatibilité moderne (par défaut)

Utilisez la stratégie par défaut si vous avez besoin d'un chiffrement fort et que vous n'avez pas d'exigences particulières. Cette stratégie est compatible avec la plupart des clients TLS et SSH.

Compatibilité héritée

Utilisez la stratégie de compatibilité héritée si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette stratégie peuvent la rendre moins sécurisée que la stratégie de compatibilité moderne.

Critères communs

Utilisez la politique Common Criteria si vous avez besoin d'une certification Common Criteria.

FIPS strict

Utilisez la politique FIPS stricte si vous avez besoin de la certification Critères communs et devez utiliser le NetApp Cryptographic Security Module (NCSM) 3.0.8 ou le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au Tenant Manager et au Grid Manager. L'utilisation de cette politique peut réduire les performances.

Les modules NCSM 3.0.8 et NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 sont utilisés dans les opérations suivantes :

- NCSM

- Connexions TLS entre les services suivants : ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw et cache-svc
- Connexions TLS entre les clients et le service nginx-gw (points de terminaison de l'équilibreur de charge)
- Connexions TLS entre les clients et le service LDR
- Chiffrement du contenu des objets pour SSE-S3, SSE-C et le paramètre de chiffrement des objets stockés
- connexions SSH

Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "[Certificat n° 4838](#)".

- NetApp StorageGRID module API de chiffrement du noyau

Le module API de chiffrement du noyau NetApp StorageGRID est présent uniquement sur les plateformes VM et les appliances StorageGRID.

- Collecte d'entropie
- Chiffrement du nœud

Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "[Certificats n° A6242 à A6257](#)" et "[Certificat d'entropie n° E223](#)".

Remarque : Après avoir sélectionné cette stratégie, "[effectuer un redémarrage progressif](#)" pour activer le NCSM sur tous les nœuds. Utilisez **Maintenance > Redémarrage progressif** pour lancer et surveiller les redémarrages.

Personnalisé

Créez une politique personnalisée si vous devez appliquer vos propres chiffrements.

Si votre StorageGRID est soumis à des exigences de cryptographie FIPS 140, vous pouvez activer la fonctionnalité de mode FIPS pour utiliser le module NCSM 3.0.8 et le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 :

- Définissez le `fipsMode` paramètre sur `true`.
- Lorsque vous y êtes invité, "[effectuer un redémarrage progressif](#)" pour activer les modules de cryptographie sur tous les nœuds. Utilisez **Maintenance > Rolling reboot** pour lancer et surveiller les redémarrages.
- Sélectionnez **Support > Diagnostics** pour afficher les versions actives du module FIPS.

- Pour consulter les détails des chiffrements, protocoles et algorithmes de chaque politique, sélectionnez **Afficher les détails**.
- Pour modifier la politique actuelle, sélectionnez **Utiliser la politique**.

Une coche verte apparaît à côté de **Current policy** sur la vignette de la politique.

Créer une politique de sécurité personnalisée

Vous pouvez créer une politique personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

- À partir de la vignette de la politique la plus similaire à la politique personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
- Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.



- Dans la vignette **Stratégie personnalisée**, sélectionnez **Configurer et utiliser**.
- Collez le JSON que vous avez copié et apportez les modifications nécessaires.
- Sélectionnez **Utiliser la stratégie**.

Une coche verte apparaît à côté de **Police actuelle** sur la vignette **Police personnalisée**.

6. Vous pouvez également sélectionner **Modifier la configuration** pour apporter d'autres modifications à la nouvelle politique personnalisée.

Rétablir temporairement la politique de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, vous pourriez ne pas être en mesure de vous connecter au Grid Manager si la stratégie TLS configurée est incompatible avec le ["certificat de serveur configuré"](#).

Vous pouvez temporairement rétablir la politique de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
 - c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
 - d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

2. Exécutez la commande suivante :

```
restore-default-cipher-configurations
```

3. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.
4. Suivez les étapes décrites dans [Sélectionnez une politique de sécurité](#) pour configurer à nouveau la politique.

Configurer la sécurité du réseau et des objets StorageGRID

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, empêcher certaines requêtes S3 ou autoriser les connexions client aux Storage Nodes à utiliser HTTP au lieu de HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données des objets lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de chiffrement AES-128 ou AES-256. Lorsque vous activez ce paramètre, tous les nouveaux objets ingérés sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les nouveaux objets ingérés ne sont pas chiffrés.

Le paramètre de chiffrement des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID, voir ["Passez en revue les méthodes de chiffrement de StorageGRID"](#).

Empêcher la modification du client

Empêcher la modification par le client est un paramètre à l'échelle du système. Lorsque l'option **Empêcher la modification par le client** est sélectionnée, les requêtes suivantes sont refusées.

API REST S3

- DeleteBucket demandes
- Toute demande de modification des données, des métadonnées définies par l'utilisateur ou du balisage d'objet S3 existant

Activer HTTP pour les connexions au nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toute connexion directe aux Storage Nodes. Vous pouvez activer le protocole HTTP pour ces connexions, par exemple lors du test d'une grille hors production.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 doivent établir des connexions HTTP directes avec ces nœuds. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (car vous pouvez ["configurer chaque point de terminaison d'équilibrage de charge"](#) utiliser HTTP ou HTTPS).

Consultez ["Résumé : adresses IP et ports pour les connexions client"](#) pour savoir quels ports les clients S3 utilisent lorsqu'ils se connectent aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous disposez des droits d'accès root.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **Réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **Aucun** (par défaut) si vous ne souhaitez pas que les objets stockés soient chiffrés, ou sélectionnez **AES-128** ou **AES-256** pour chiffrer les objets stockés.
4. Vous pouvez également sélectionner **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des requêtes spécifiques.



Si vous modifiez ce paramètre, il faudra environ une minute pour que le nouveau paramètre soit appliqué. La valeur configurée est mise en cache pour optimiser les performances et la mise à l'échelle.

5. Vous pouvez également sélectionner **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.



Soyez prudent lorsque vous activez le protocole HTTP pour une grille de production, car les requêtes seront envoyées sans chiffrement.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface StorageGRID

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant une durée supérieure à celle spécifiée et si une trace de pile est incluse dans les réponses d'erreur de l'API.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["Autorisation d'accès root"](#).

À propos de cette tâche

La page **Paramètres de sécurité** comprend les paramètres **Délai d'inactivité du navigateur** et **Trace de pile de l'API de gestion**.

Délai d'inactivité du navigateur

Indique la durée pendant laquelle le navigateur d'un utilisateur peut rester inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est de 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID distinct et non configurable est inclus pour la sécurité du système. Le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'inactivité du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique (SSO) soit activée pour StorageGRID.

Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur expire, ce dernier doit saisir à nouveau ses identifiants SSO pour accéder de nouveau à StorageGRID. Voir ["Fonctionnement de l'authentification unique \(SSO\)"](#).

Trace de pile de l'API de gestion

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur des API Grid Manager et Tenant Manager.

Cette option est désactivée par défaut, mais vous pouvez activer cette fonctionnalité pour un environnement de test. En règle générale, vous devez laisser la trace de pile désactivée dans les environnements de production afin d'éviter de révéler des détails internes du logiciel lorsque des erreurs d'API se produisent.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
 - a. Déployez l'accordéon.
 - b. Pour modifier le délai d'expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d'expiration par défaut est de 15 minutes.

- c. Pour désactiver cette fonctionnalité, décochez la case.
- d. Sélectionnez **Enregistrer**.

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

- 4. Pour modifier le paramètre de trace de pile de l'API de gestion :
 - a. Déployez l'accordéon.
 - b. Cochez la case pour afficher une trace de pile dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.



Laissez la trace de pile désactivée dans les environnements de production afin d'éviter de révéler des détails internes du logiciel en cas d'erreurs d'API.

- c. Sélectionnez **Enregistrer**.

Gérer l'accès SSH externe dans StorageGRID

Gérez l'accès SSH au trafic entrant dans la grille en bloquant ou en autorisant l'accès externe. La gestion de l'accès SSH externe n'a aucun impact sur le trafic entre les nœuds de la grille.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["Autorisation d'accès root"](#).

À propos de cette tâche

Pour renforcer la sécurité du système, l'accès SSH externe est bloqué par défaut. Si vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage, autorisez temporairement l'accès externe. Lorsque vous avez terminé la tâche, bloquez l'accès externe.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **Bloquer SSH**.
3. Utilisez l'option **Bloquer l'accès SSH entrant** pour gérer l'accès SSH externe :
 - a. Cochez la case pour bloquer l'accès (par défaut).
 - b. Décochez la case pour autoriser l'accès.



Nécessite un accès au port 22 entre l'ordinateur portable de service et tous les autres nœuds du grid. Supprimez l'accès au port 22 une fois la tâche de maintenance terminée.

4. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion des clés

Découvrez les serveurs de gestion des clés dans StorageGRID

Un serveur de gestion de clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé en utilisant le protocole d'interopérabilité de gestion de clés (KMIP).

StorageGRID ne prend en charge que certains serveurs de gestion de clés. Pour obtenir la liste des produits et des versions pris en charge, utilisez le ["Outil de matrice d'interopérabilité \(IMT\) NetApp"](#).

Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement des nœuds StorageGRID dont l'option **Chiffrement des nœuds** est activée lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds StorageGRID vous permet de protéger vos données même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif, sauf si le nœud peut communiquer avec le KMS.

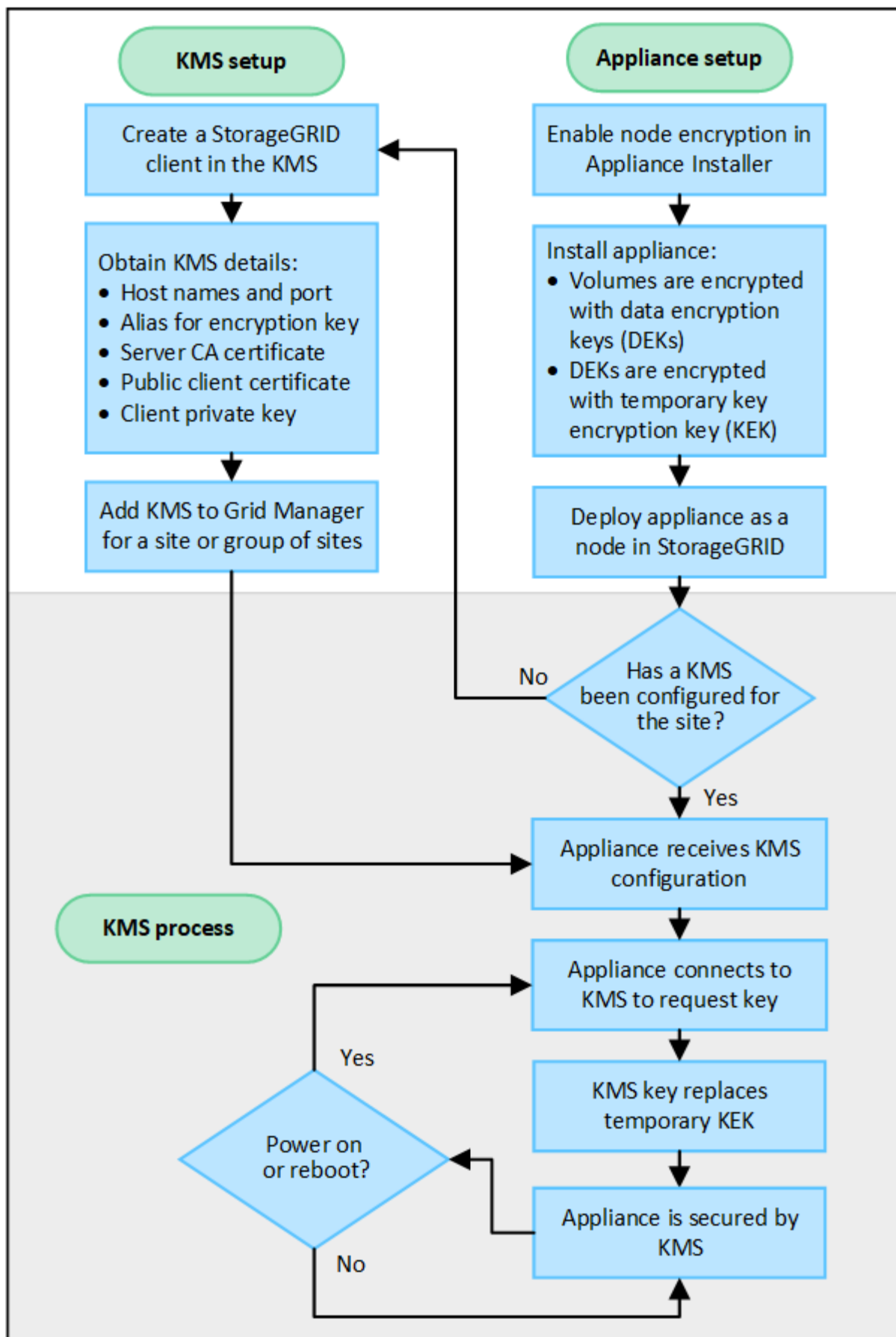


StorageGRID ne crée ni ne gère les clés externes utilisées pour chiffrer et déchiffrer les nœuds de l'appliance. Si vous prévoyez d'utiliser un serveur de gestion de clés externe pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et comment gérer les clés de chiffrement. L'exécution des tâches de gestion des clés dépasse le cadre de ces instructions. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion de clés ou contactez le support technique.

Configuration du serveur de gestion des clés et de l'appliance StorageGRID

Avant de pouvoir utiliser un serveur de gestion de clés (KMS) pour sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés s'effectue automatiquement.

Le diagramme illustre les grandes étapes de l'utilisation d'un KMS pour sécuriser les données StorageGRID sur les nœuds de l'appliance.



Le diagramme montre que la configuration du KMS et celle de l'appliance se déroulent en parallèle ;

cependant, vous pouvez configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement pour les nouveaux nœuds de l'appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La mise en place d'un serveur de gestion de clés comprend les étapes générales suivantes.

Étape	Consultez
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurez StorageGRID en tant que client dans le KMS"
Obtenez les informations requises pour le client StorageGRID sur le KMS.	"Configurez StorageGRID en tant que client dans le KMS"
Ajoutez le KMS au Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléversez les certificats requis et enregistrez la configuration du KMS.	"Ajouter un serveur de gestion de clés (KMS)"

Configurez l'appareil

La configuration d'un nœud d'appliance pour une utilisation KMS comprend les étapes générales suivantes.

1. Lors de la phase de configuration matérielle de l'installation de l'appliance, utilisez le StorageGRID Appliance Installer pour activer le paramètre **Chiffrement de nœud** pour l'appliance.



Vous ne pouvez pas activer le paramètre **Chiffrement des nœuds** après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion de clés externes pour les appareils qui n'ont pas le chiffrement des nœuds activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement de données (DEK) aléatoire est attribuée à chaque volume de l'appliance, comme suit :
 - Les clés DEK servent à chiffrer les données de chaque volume. Ces clés sont générées à l'aide du chiffrement de disque Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
 - Chaque DEK individuel est chiffré par une clé de chiffrement principale (KEK). La KEK initiale est une clé temporaire qui chiffre les DEK jusqu'à ce que l'appliance puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

Voir ["Activer le chiffrement des nœuds"](#) pour plus de détails.

Processus de chiffrement de la gestion des clés (effectué automatiquement)

Le chiffrement avec gestion des clés comprend les étapes générales suivantes, qui sont exécutées automatiquement.

1. Lorsque vous installez dans la grille un appareil dont le chiffrement des nœuds est activé, 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 aucun KMS n'a encore été configuré pour le site, les données sur l'apppliance continuent d'être chiffrées par la KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'apppliance reçoive la configuration KMS.
2. L'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
 3. Le KMS envoie une clé de chiffrement à l'apppliance. La nouvelle clé provenant du KMS remplace la clé KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les clés DEK des volumes de l'apppliance.



Toutes les données existantes avant la connexion du nœud de l'apppliance chiffrée au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'apppliance ne doivent pas être considérés comme protégés contre leur suppression du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

4. Si l'appareil est mis sous tension ou redémarré, il se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée en mémoire volatile, ne peut pas survivre à une coupure de courant ou à un redémarrage.

Exigences et considérations relatives au serveur de gestion des clés StorageGRID

Avant de configurer un serveur de gestion de clés externe (KMS), vous devez comprendre les considérations et les exigences.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

["Spécification du protocole d'interopérabilité de gestion des clés, version 1.4"](#)

Quelles sont les considérations relatives au réseau ?

Les paramètres du pare-feu réseau doivent autoriser chaque nœud de l'apppliance à communiquer via le port utilisé pour le protocole Key Management Interoperability Protocol (KMIP). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'apppliance utilisant le chiffrement dispose d'un accès réseau au KMS ou au cluster KMS que vous avez configuré pour le site.

Quelles versions de TLS sont prises en charge ?

Les communications entre les nœuds de l'apppliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID peut prendre en charge soit le protocole TLS 1.2, soit le protocole TLS 1.3 lors des connexions KMIP à un KMS ou un cluster KMS, en fonction de ce que le KMS prend en charge et de celui que ["Politique TLS et SSH"](#) vous utilisez.

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lors de l'établissement de la connexion. Pour connaître les versions de protocole et les chiffrements/suites de chiffrement disponibles, consultez la `tlsOutbound` section de la politique TLS et SSH active de la grille (**Configuration > Sécurité Paramètres de sécurité**).

Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout appareil StorageGRID de votre grille dont l'option **Chiffrement des nœuds** est activée. Cette option ne peut être activée que lors de l'étape de configuration matérielle de l'installation de l'appareil, à l'aide de l'outil StorageGRID Appliance Installer.



Vous ne pouvez pas activer le chiffrement du nœud après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion externe des clés pour les appareils qui n'ont pas le chiffrement du nœud activé.

Vous pouvez utiliser le KMS configuré pour les appliances StorageGRID et les nœuds d'appliance.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non-appliance), notamment les suivants :

- Nœuds déployés en tant que machines virtuelles (VM)
- Nœuds déployés au sein de moteurs de conteneurs sur des hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Lors d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion de clés dans Grid Manager avant de créer des locataires. Cet ordre garantit que les nœuds sont protégés avant que des données d'objets ne soient stockées dessus.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

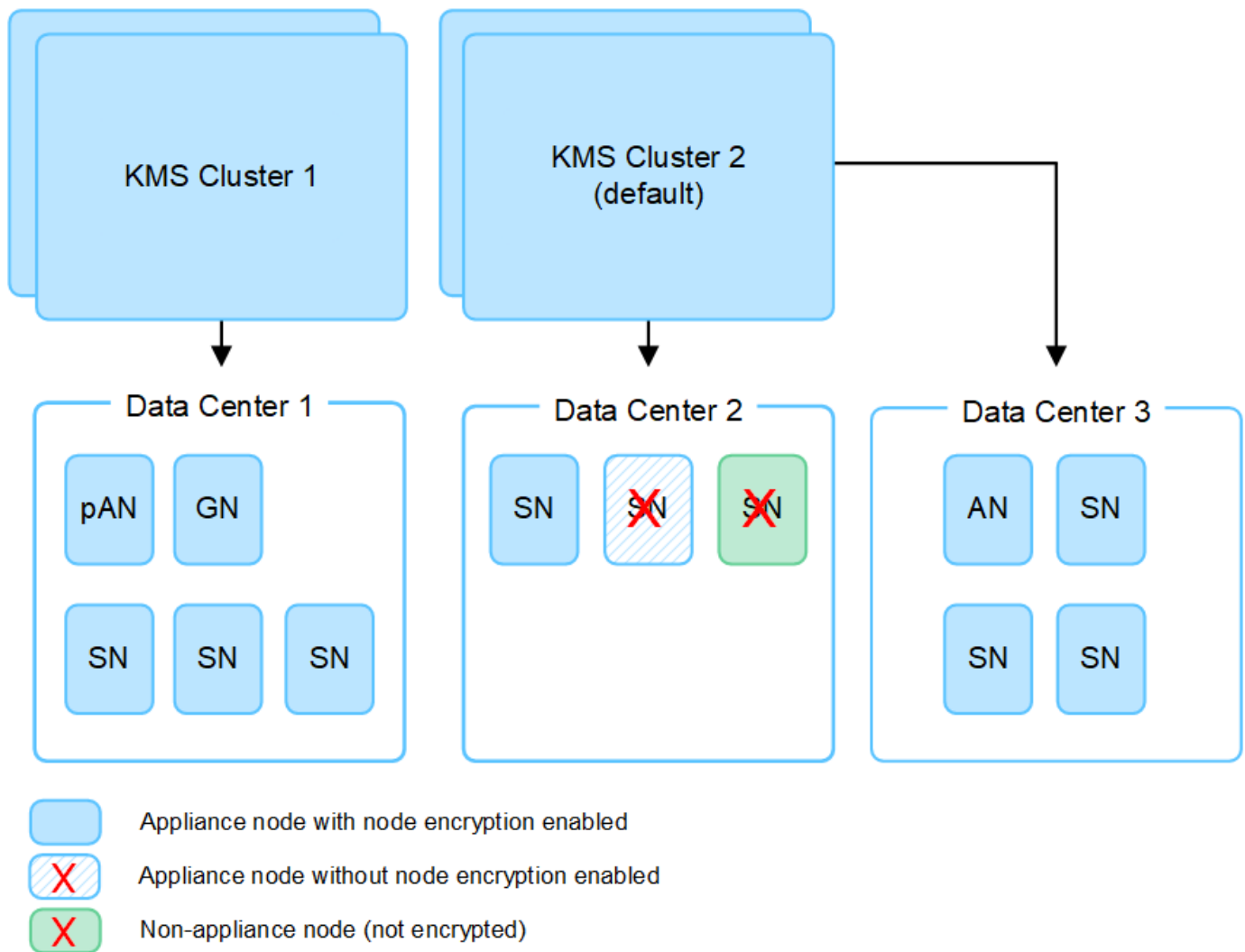
De combien de serveurs de gestion de clés avez-vous besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion de clés externes pour fournir des clés de chiffrement aux nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une seule clé de chiffrement aux nœuds d'appliance StorageGRID d'un site ou d'un groupe de sites.

StorageGRID prend en charge l'utilisation de clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion de clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée car elle améliore les capacités de basculement d'une configuration à haute disponibilité.

Par exemple, supposons que votre système StorageGRID comporte trois centres de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du Data Center 1 et un second cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous 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 un KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Node Encryption** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que bonne pratique de sécurité, vous devez périodiquement ["faites pivoter la clé de chiffrement"](#) utilisée par chaque KMS configuré.

Lorsque la nouvelle version de la clé sera disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés du ou des sites associés au KMS. La distribution doit avoir lieu dans l'heure suivant la rotation de la clé.
- Si le nœud de l'appliance chiffrée est hors ligne lors de la distribution de la nouvelle version de la clé, il recevra la nouvelle clé dès son redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour quelque raison que ce soit, l'alerte **KMS encryption key rotation failed** 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 son chiffrement ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID, vous devez d'abord mettre hors service le nœud de la grille afin de déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le StorageGRID Appliance Installer ["effacer la configuration KMS"](#). La suppression de la

configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud du dispositif et la configuration KMS pour le site StorageGRID.



Sans accès à la clé de chiffrement KMS, toutes les données restant sur l'appareil ne peuvent plus être accessibles et sont définitivement verrouillées.

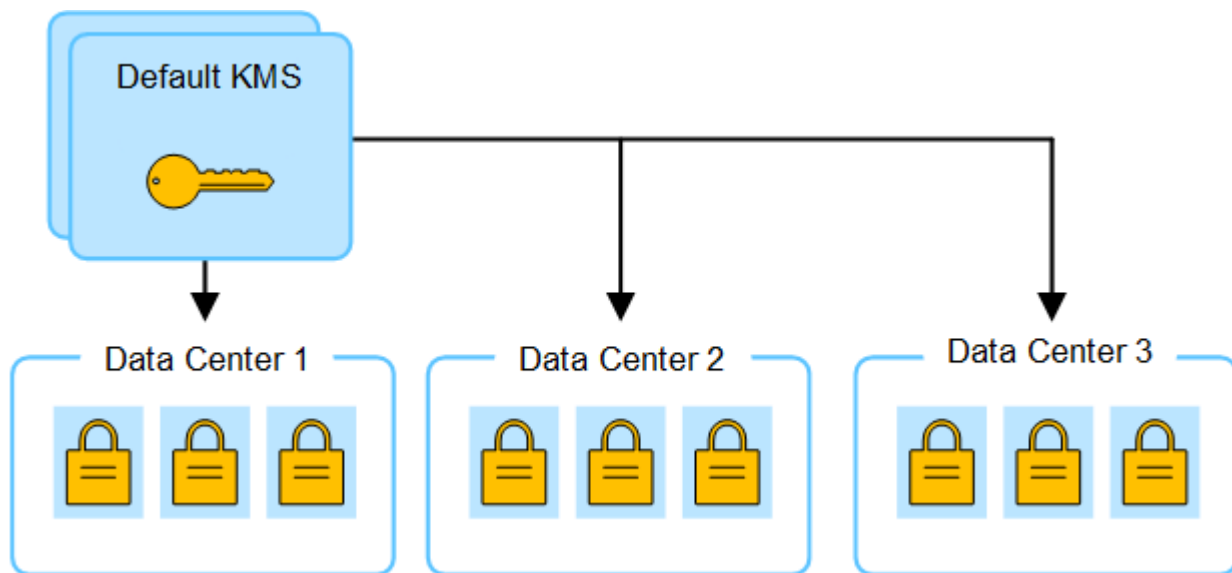
Considérations relatives à la modification du KMS pour un site StorageGRID

Chaque serveur de gestion de clés (KMS) ou cluster KMS fournit une clé de chiffrement à tous les nœuds d'appliance d'un site ou d'un groupe de sites. Si vous devez changer le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS à un autre.

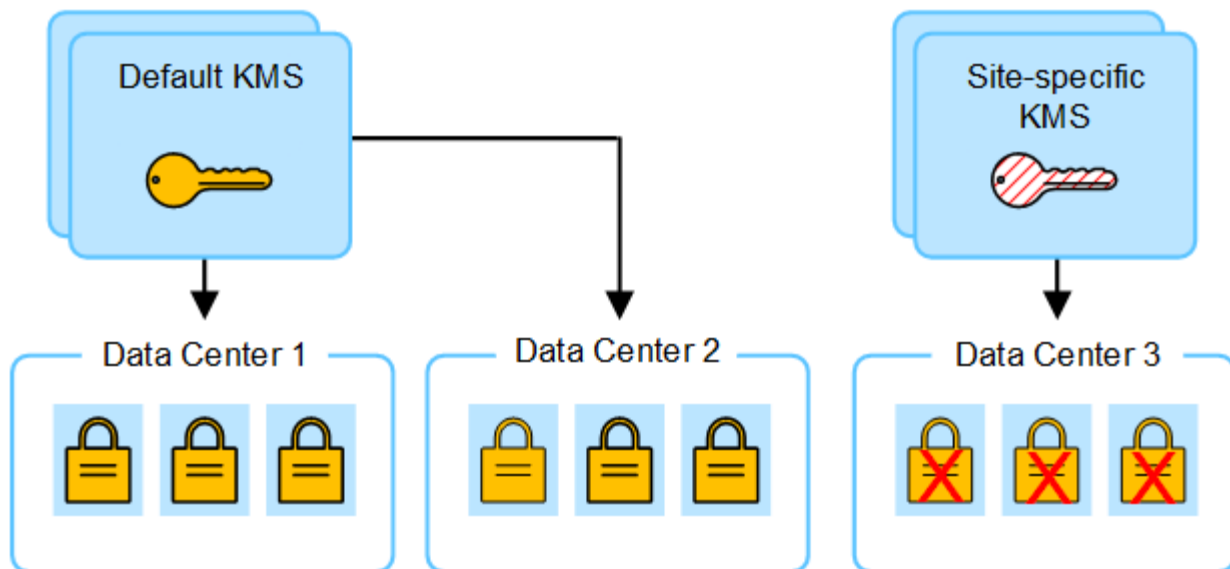
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous pourriez avoir besoin de copier la version actuelle de la clé de chiffrement du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS possède la clé correcte pour déchiffrer les nœuds d'appliance chiffrés sur le site.

Par exemple :

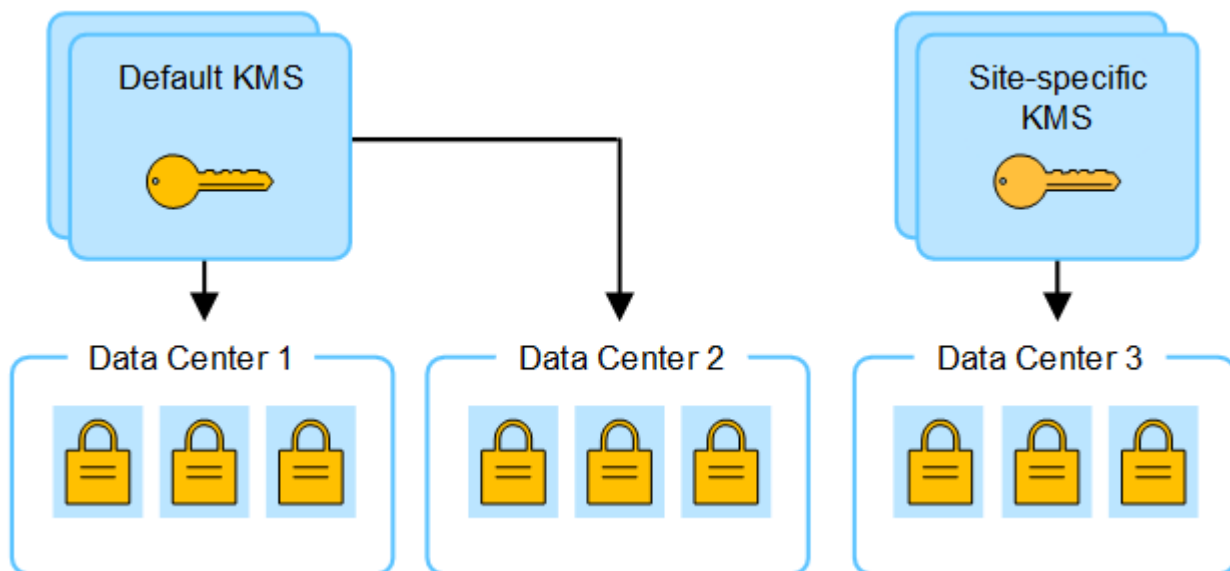
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites ne disposant pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement des nœuds** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds d'appliance sur tous les sites. Cette même clé doit également être utilisée pour déchiffrer ces appliances.



3. Vous décidez d'ajouter un KMS spécifique au site (Data Center 3 sur la figure). Cependant, comme les nœuds de l'appliance sont déjà chiffrés, une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit parce que le KMS spécifique au site ne possède pas la clé correcte pour déchiffrer les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine vers une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour déchiffrer les nœuds de l'appliance du Data Center 3, elle peut donc être enregistrée dans StorageGRID.



Cas d'utilisation pour la modification du KMS utilisé pour un site

Le tableau récapitule les étapes nécessaires pour les cas les plus courants de modification du KMS d'un site.

Cas d'utilisation pour la modification du KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez en utiliser une comme KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ Gère les clés pour, sélectionnez Sites non gérés par un autre KMS (KMS par défaut). Le KMS spécifique au site sera désormais utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'un KMS par défaut et vous ajoutez un nouveau site lors d'une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds de l'appliance sur le nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS par défaut vers un nouveau KMS. 2. À l'aide du Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajouter un serveur de gestion de clés (KMS)"
Vous souhaitez que le KMS d'un site utilise un serveur différent.	1. Si les nœuds de l'appliance sur le site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS existant vers le nouveau KMS. 2. À l'aide du Grid Manager, modifiez la configuration KMS existante et saisissez le nouveau nom de l'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurez StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion de clés externe ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.



Ces instructions s'appliquent à Thales CipherTrust Manager et Hashicorp Vault. Pour obtenir la liste des produits et versions compatibles, utilisez le ["Outil de matrice d'interopérabilité \(IMT\) NetApp"](#).

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque KMS ou cluster KMS que vous prévoyez d'utiliser.

Chaque KMS gère une seule clé de chiffrement pour les nœuds des appliances StorageGRID sur un seul site ou sur un groupe de sites.

2. Créez une clé en utilisant l'une des deux méthodes suivantes :

- Utilisez la page de gestion des clés de votre produit KMS. Créez une clé de chiffrement AES pour chaque KMS ou cluster KMS.

La clé de chiffrement doit comporter au moins 2 048 bits et être exportable.

- Laissez StorageGRID créer la clé. Vous serez invité à le faire lors du test et de l'enregistrement après ["téléversement des certificats clients"](#).

3. Enregistrez les informations suivantes pour chaque KMS ou cluster KMS.

Vous aurez besoin de ces informations lorsque vous ajouterez le KMS à StorageGRID :

- Nom d'hôte ou adresse IP pour chaque serveur.
 - Port KMIP utilisé par le KMS.
 - Alias de la clé de chiffrement dans le KMS.
4. Pour chaque KMS ou cluster KMS, obtenez un certificat serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA encodés au format 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 en Base-64 Privacy Enhanced Mail (PEM).
- Le champ Subject Alternative Name (SAN) de chaque certificat de serveur doit inclure le domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.



Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir 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. Obtenez le certificat client public délivré à StorageGRID par le KMS externe et la clé privée du certificat client.

Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés dans StorageGRID

Vous utilisez l'assistant du serveur de gestion de clés StorageGRID pour ajouter chaque KMS ou cluster KMS.

Avant de commencer

- Vous avez examiné le ["Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés"](#).
- Vous avez ["configuré StorageGRID comme client dans le KMS"](#), et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

À propos de cette tâche

Si possible, configurez les serveurs de gestion de clés spécifiques à chaque site avant de configurer un KMS par défaut applicable à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, tous les équipements chiffrés au niveau des nœuds dans la grille seront chiffrés par le KMS par défaut. Si vous souhaitez créer un KMS spécifique à un site ultérieurement, vous devez d'abord copier la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. Voir ["Considérations relatives à la modification du KMS d'un site"](#) pour plus de détails.

Étape 1 : Détails du KMS

À l'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés, vous fournissez des détails sur le KMS ou le cluster KMS.

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.

La page du serveur de gestion des clés s'affiche avec l'onglet Détails de la configuration sélectionné.

2. Sélectionnez **Create**.

L'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés apparaît.

3. Saisissez les informations suivantes concernant le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Remarque : Si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer les serveurs de gestion de clés spécifiques à un site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS doit gérer les clés de chiffrement des 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 ne disposant pas d'un KMS dédié et à tous les sites que vous ajouterez lors d'extensions ultérieures. Remarque : Une erreur de validation se produira lors de l'enregistrement de la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS.
Port	Le port que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.

Champ	Description
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. Remarque : Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni à tous les serveurs d'un cluster KMS.

- Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
- Sélectionnez **Continue**.

Étape 2 : Télécharger le certificat du serveur

À l'étape 2 (Téléchargement du certificat serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat serveur (ou le lot de certificats) pour le KMS. Le certificat serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

- À partir de l'**étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat du serveur enregistré ou du bundle de certificats.
- Téléchargez le fichier de certificat.

Les métadonnées du certificat du serveur apparaissent.



Si vous avez importé un ensemble de certificats, les métadonnées de chaque certificat apparaissent dans son propre onglet.

- Sélectionnez **Continue**.

Étape 3 : Téléversez les certificats clients

À l'étape 3 (Téléchargement des certificats clients) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

- À partir de l'**étape 3 (Télécharger les certificats clients)**, accédez à l'emplacement du certificat client.
- Téléchargez le fichier de certificat client.

Les métadonnées du certificat client apparaissent.

- Accédez à l'emplacement de la clé privée du certificat client.
- Téléversez le fichier de clé privée.
- Sélectionnez **Tester et enregistrer**.

Si aucune clé n'existe, vous êtes invité à laisser StorageGRID en créer une.

Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des

clés est ajouté au tableau 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. StorageGRID peut prendre jusqu'à 30 minutes pour obtenir l'état réel de chaque certificat. Vous devez actualiser votre navigateur web pour voir l'état actuel.

6. Si un message d'erreur apparaît lorsque vous sélectionnez **Tester et enregistrer**, consultez les détails du message, puis sélectionnez **OK**.

Par exemple, vous pourriez recevoir une erreur 422 : Entité non traitable si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **Forcer l'enregistrement**.



L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

8. Examinez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Gérer un serveur de gestion de clés dans StorageGRID

La gestion d'un serveur de gestion de clés (KMS) implique la consultation ou la modification des détails, la gestion des certificats, la consultation des nœuds chiffrés et la suppression d'un KMS lorsqu'il n'est plus nécessaire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisation d'accès requise"](#).

Afficher les détails KMS

Vous pouvez consulter les informations relatives à chaque serveur de gestion de clés (KMS) dans votre système StorageGRID, notamment les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.

La page du serveur de gestion des clés s'affiche et présente les informations suivantes :

- L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.
- L'onglet « Nœuds chiffrés » répertorie tous les nœuds dont le chiffrement de nœud est activé.

2. Pour consulter les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS affiche les informations suivantes :

Champ	Description
Gère les clés pour	Le site StorageGRID associé au KMS. Ce champ affiche le nom d'un site StorageGRID spécifique ou des sites non gérés par un autre KMS (KMS par défaut).
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion de clés, le domaine complet ou l'adresse IP des deux serveurs est indiqué. S'il existe plus de deux serveurs de gestion de clés dans un cluster, le domaine complet ou l'adresse IP du premier KMS est indiqué, ainsi que le nombre de serveurs de gestion de clés supplémentaires dans le cluster. Par exemple : 10.10.10.10 and 10.10.10.11 ou 10.10.10.10 and 2 others. Pour afficher tous les noms d'hôte d'un cluster, sélectionnez un KMS et sélectionnez Modifier ou Actions > Modifier.

3. Sélectionnez un onglet sur la page de détails KMS pour afficher les informations suivantes :

Onglet	Champ	Description
Détails clés	Nom de la clé	L'alias de clé pour le client StorageGRID dans le KMS.
UID de la clé	L'identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration, et le certificat PEM.	Certificat PEM	Le contenu du fichier PEM (privacy enhanced mail) pour le certificat.
Certificat client	Métadonnées	Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration, et le certificat PEM.

4. Aussi souvent que nécessaire selon les pratiques de sécurité de votre organisation, sélectionnez **Rotate key** ou utilisez le logiciel KMS pour créer une nouvelle version de la clé.

Lorsque la rotation de la clé réussit, les champs Key UID et Dernière modification sont mis à jour.

Si vous faites pivoter la clé de chiffrement à l'aide du logiciel KMS, faites-la pivoter de la dernière version utilisée de la clé vers une nouvelle version de cette même clé. Ne faites pas pivoter vers une clé totalement différente.



Ne tentez jamais de faire tourner une clé en modifiant son nom (alias) auprès du KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID pourrait ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Réglez rapidement tout problème lié aux certificats serveur ou client. Si possible, remplacez les certificats avant leur expiration.



Vous devez régler tout problème de certificat dès que possible afin de maintenir l'accès aux données.

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.
2. Dans le tableau, consultez la valeur de l'expiration du certificat pour chaque KMS.
3. Si la date d'expiration du certificat de n'importe quel KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur web.
4. Si la colonne « Expiration du certificat » indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page de détails du KMS.
 - a. Sélectionnez **Certificat serveur** et vérifiez la valeur du champ « Expire le ».
 - b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
 - c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de **Certificat serveur**.
5. Lorsque les alertes **KMS CA certificate expiration**, **KMS client certificate expiration** et **KMS server certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

StorageGRID peut prendre jusqu'à 30 minutes pour mettre à jour la date d'expiration du certificat. Actualisez votre navigateur web pour voir les valeurs actuelles.



Si vous obtenez le statut **Statut du certificat serveur inconnu**, assurez-vous que votre KMS permette d'obtenir un certificat serveur sans exiger de certificat client.

Afficher les nœuds chiffrés

Vous pouvez consulter les informations relatives aux nœuds d'appliance de votre système StorageGRID dont le paramètre **Chiffrement des nœuds** est activé.

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.

La page Serveur de gestion des clés s'affiche. L'onglet Détails de la configuration présente les serveurs de gestion des clés configurés.

2. En haut de la page, sélectionnez l'onglet **Nœuds chiffrés**.

L'onglet Nœuds chiffrés répertorie les nœuds d'appliance de votre système StorageGRID dont le paramètre **Chiffrement des nœuds** est activé.

3. Consultez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Le nom du nœud de l'appliance.
Type de nœud	Le type de nœud : Storage, Admin ou Gateway.
Site	Le nom du site StorageGRID où le nœud est installé.
Nom KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS. "Ajouter un serveur de gestion de clés (KMS)"
UID de la clé	L'identifiant unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID complet de la clé, sélectionnez le texte. Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
Statut	État de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de la connexion peut prendre plusieurs minutes après une modification de la configuration du KMS. Remarque : Actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne « Status » indique un problème KMS, résolvez le problème immédiatement.

Lors des opérations normales du KMS, le statut sera **Connecté au KMS**. Si un nœud est déconnecté du grid, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

D'autres messages d'état correspondent à des alertes StorageGRID portant les mêmes noms :

- Échec du chargement de la configuration KMS
- Erreur de connectivité KMS
- Nom de clé de chiffrement KMS introuvable
- La rotation de la clé de chiffrement KMS a échoué
- La clé KMS n'a pas pu déchiffrer le volume de l'appliance.
- KMS n'est pas configuré

Veillez effectuer les actions recommandées pour ces alertes.



Vous devez remédier immédiatement à tout problème afin de garantir la protection intégrale de vos données.

Modifier un KMS

Vous pourriez avoir besoin de modifier la configuration d'un serveur de gestion de clés, par exemple si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le ["considérations relatives à la modification du KMS d'un site"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.

La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

2. Sélectionnez le KMS que vous souhaitez modifier, puis sélectionnez **Actions > Edit**.

Vous pouvez également modifier un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Modifier** sur la page de détails du KMS.

3. Vous pouvez également mettre à jour les détails à l'étape 1 (détails KMS) de l'assistant Modifier un Key Management Server.

Champ	Description
Nom KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Vous n'avez besoin de modifier le nom de la clé que dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de l'ancienne clé ont été copiées dans l'historique des versions du nouvel alias.

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous n'avez pas encore de KMS par défaut, vous pouvez sélectionner Sites non gérés par un autre KMS (KMS par défaut). Cette sélection convertit un KMS spécifique à un 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 lors d'une extension. Remarque : Si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. Remarque : Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.

5. Sélectionnez **Continue**.

L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un Key Management Server apparaît.

6. Si vous devez remplacer le certificat du serveur, sélectionnez **Parcourir** et importez le nouveau fichier.

7. Sélectionnez **Continue**.

L'étape 3 (Télécharger les certificats clients) de l'assistant Modifier un serveur de gestion de clés apparaît.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléversez les nouveaux fichiers.

9. Sélectionnez **Tester et enregistrer**.

Les connexions entre le serveur de gestion des clés et tous les nœuds des appliances chiffrées sur les sites concernés 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 au tableau de la page Serveur de gestion des clés.

10. Si un message d'erreur apparaît, consultez les détails du message et sélectionnez **OK**.

Par exemple, vous pourriez recevoir une erreur 422 : Entité non traitable si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **Force save**.



L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

La configuration KMS est enregistrée.

12. Examinez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Supprimer un serveur de gestion de clés (KMS)

Vous pourriez vouloir supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous pourriez vouloir supprimer un KMS spécifique à un site si vous avez mis ce site hors service.

Avant de commencer

- Vous avez examiné le "[Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".

À propos de cette tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique à un site si celui-ci a été mis hors service ou s'il ne comprend aucun nœud d'appliance avec chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site comportant des nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **Configuration > Security > Key management server**.

La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

2. Sélectionnez le KMS que vous souhaitez supprimer, puis sélectionnez **Actions > Remove**.

Vous pouvez également supprimer un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Supprimer** sur la page de détails du KMS.

3. Veuillez confirmer que ce qui suit est vrai :
 - Vous supprimez un KMS spécifique à un site pour un site qui ne possède aucun nœud d'appliance avec chiffrement de nœud activé.
 - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement de nœud.
4. Sélectionnez **Oui**.

La configuration KMS est supprimée.

Gérer les paramètres du proxy

Configurer un proxy de stockage StorageGRID

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les points de terminaison S3 externes. Par exemple, vous pourriez avoir besoin d'un proxy non transparent pour permettre l'envoi de messages des services de plateforme vers des points de terminaison externes, tels qu'un point de terminaison sur Internet.



Les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy de stockage.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres du proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

Laissez ce champ vide pour utiliser le port par défaut du protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

Une fois le proxy de stockage enregistré, de nouveaux points de terminaison pour les services de plateforme ou les Cloud Storage Pools peuvent être configurés et testés.



Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plateforme provenant de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurez les paramètres du proxy d'administration dans StorageGRID

Si vous envoyez des packages AutoSupport en utilisant HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Pour plus d'informations sur AutoSupport, voir "[Configurez AutoSupport](#)".

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy d'administration.

Étapes

1. Sélectionnez **Configuration > Sécurité > Paramètres du proxy**.

La page Paramètres du proxy s'affiche. Par défaut, Stockage est sélectionné dans le menu des onglets.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy d'administration**.
4. Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Saisissez le port utilisé pour vous connecter au serveur proxy.
6. Vous pouvez éventuellement saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

Laissez ces champs vides si votre serveur proxy ne requiert ni nom d'utilisateur ni mot de passe.

7. Sélectionnez l'une des options suivantes :

- Pour sécuriser la connexion au proxy d'administration, sélectionnez **Vérifier le certificat du proxy**. Chargez un bundle CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.



AutoSupport on Demand, E-Series AutoSupport via StorageGRID, et la détermination du chemin de mise à jour sur la page de mise à niveau StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Après que vous ayez téléchargé le paquet CA, ses métadonnées apparaissent.

- Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **Ne pas vérifier le certificat proxy**.

8. Sélectionnez **Enregistrer**.

Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.



Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

9. Si vous devez désactiver le proxy d'administration, décochez la case **Activer le proxy d'administration**, puis sélectionnez **Enregistrer**.

Contrôlez les pare-feu

Contrôlez l'accès à StorageGRID à un pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API sur les nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du pare-feu externe. Par exemple,

vous pouvez empêcher les locataires de se connecter au Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne de StorageGRID, consultez "[Configurer le pare-feu interne](#)".

Port	Description	Si le port est ouvert...
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager, à l'API de gestion du Grid, au Tenant Manager et à l'API de gestion du Tenant. Remarque : Le port 443 est également utilisé pour une partie du trafic interne.
8443	Port restreint du Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager et à l'API de gestion du Grid à l'aide de HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder au Tenant Manager ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port restreint du gestionnaire de locataires sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Tenant Manager 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 au Grid Manager ni à l'API de gestion du Grid. • Les demandes de contenu interne seront rejetées.



L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- "[Connectez-vous au Grid Manager](#)"
- "[Créer un compte locataire](#)"
- "[Communications externes](#)"

Gérez les contrôles de pare-feu internes dans StorageGRID

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grid en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès réseau sur tous les ports, sauf ceux nécessaires au déploiement spécifique de votre grid. Les modifications de configuration que vous

effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grid.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès à des ports fermés sélectionnés. Vous pouvez ajouter des adresses IP ou des sous-réseaux au format CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet Gérer l'accès externe.
- **Gérer l'accès externe** : Utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : Utilisez cet onglet pour spécifier si un nœud fait confiance au trafic entrant provenant du réseau client.

Les paramètres de cet onglet prévalent sur ceux de l'onglet Gérer l'accès externe.

- Un nœud doté d'un Client Network non fiable n'acceptera que les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et liés au type de nœud).
- Les ports des points de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Manage external networks.
- Une fois approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.



Les paramètres que vous définissez dans un onglet peuvent affecter les modifications d'accès que vous effectuez dans un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, consultez ["Configurer les contrôles du pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez ["Contrôler l'accès au niveau du pare-feu externe"](#).

Onglets Liste d'adresses privilégiées et Gérer l'accès externe

L'onglet « Liste des adresses privilégiées » vous permet d'enregistrer une ou plusieurs adresses IP autorisées à accéder à des ports de la grille fermés. L'onglet « Gérer l'accès externe » vous permet de fermer l'accès externe à certains ports externes ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut aux nœuds non-grille). Ces deux onglets peuvent souvent être utilisés conjointement pour personnaliser précisément l'accès réseau dont vous avez besoin pour votre grille.



Les adresses IP privilégiées n'ont pas accès par défaut aux ports internes de la grille.

Exemple 1 : Utilisez un serveur de rebond pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un serveur de rebond (un hôte sécurisé) pour l'administration du réseau. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste des adresses privilégiées pour ajouter l'adresse IP de l'hôte de rebond.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.



Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception du jump host. Vous pouvez alors utiliser le jump host pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : Verrouillez les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour n'accorder l'accès qu'aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.



Ajoutez l'adresse IP privilégiée avant de bloquer l'accès à tout port attribué à l'accès à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tout utilisateur actuellement connecté à un port bloqué, y compris vous, perdra l'accès à Grid Manager à moins que son adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, le port sensible et le service associé sont accessibles aux hôtes figurant dans la liste d'adresses privilégiées. L'accès au service est refusé à tous les autres hôtes, quelle que soit l'interface d'où provient la requête.

Exemple 3 : Désactivez l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, pour bloquer le trafic HTTP des clients S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en n'acceptant le trafic client entrant que sur les points de terminaison explicitement configurés.

Par défaut, le réseau client de chaque nœud de la grille est *de confiance*. Autrement dit, par défaut, StorageGRID fait confiance aux connexions entrantes vers chaque nœud de la grille sur tous les ["ports externes disponibles"](#).

Vous pouvez réduire le risque d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client de chaque nœud soit *non fiable*. Si le réseau client d'un nœud est non fiable, le nœud n'accepte les connexions entrantes que sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir ["Configurer les points de terminaison de l'équilibreur de charge"](#) et ["Configurer les contrôles du pare-feu"](#).

Exemple 1 : Le nœud passerelle accepte uniquement les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud Gateway refuse tout le trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous effectueriez les étapes générales suivantes :

1. À partir de la page ["points de terminaison de l'équilibreur de charge"](#), configurez un point de terminaison

d'équilibrage de charge pour S3 via HTTPS sur le port 443.

2. Sur la page de contrôle du pare-feu, sélectionnez Non approuvé pour indiquer que le réseau client sur le nœud de passerelle n'est pas approuvé.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud de passerelle est bloqué, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Un nœud de stockage envoie des requêtes de services de plateforme S3

Supposons que vous souhaitiez autoriser le trafic sortant des services de la plateforme S3 depuis un nœud de stockage, mais empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez l'étape générale suivante :

- Dans l'onglet Réseaux clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas approuvé.

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les requêtes sortantes vers les destinations des services de plateforme configurés.

Exemple 3 : Limiter l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Vous effectueriez les étapes suivantes :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Untrusted Client Network pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibreur de charge d'interface de gestion, saisissez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour Réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne de StorageGRID

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez examiné les informations dans ["Gérer les contrôles du pare-feu"](#) et ["Directives de mise en réseau"](#).
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle n'accepte le trafic entrant que sur les points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.



Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

À propos de cette tâche

StorageGRID intègre un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports qui sont ouverts par défaut sur le réseau de la grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille qui sont fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud fait confiance au trafic entrant provenant du réseau client, et vous pouvez configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP extérieures à votre grid aux seuls ports strictement nécessaires renforce la sécurité de votre grid. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles du pare-feu, y compris des exemples, consultez ["Gérer les contrôles du pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez ["Contrôler l'accès au niveau du pare-feu externe"](#).

Contrôler l'accès au pare-feu

Étapes

1. Sélectionnez **Configuration > Sécurité > Contrôle du pare-feu**.

Les trois onglets de cette page sont décrits dans ["Gérer les contrôles du pare-feu"](#).

2. Sélectionnez un onglet pour configurer les contrôles du pare-feu.

Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez dans un onglet n'empêchent pas ce que vous pouvez faire dans les autres onglets ; cependant, les modifications de configuration que vous effectuez dans un onglet peuvent modifier le comportement des ports configurés dans les autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet Liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP et les sous-réseaux privilégiés n'ont pas accès au grid interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste des adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.



Les paramètres de l'onglet « Liste des adresses privilégiées » ne peuvent pas remplacer les paramètres de l'onglet « Réseau client non approuvé ».

Étapes

1. Dans l'onglet Liste des adresses privilégiées, saisissez l'adresse ou le sous-réseau IP auquel vous souhaitez accorder l'accès aux ports fermés.

2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un sous-réseau au format CIDR** pour ajouter des clients privilégiés supplémentaires.



Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID**. Voir "[Ports internes de StorageGRID](#)".



Cette option désactive certaines protections des services internes. Laissez-la désactivée si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port ne peut pas être accessible par une adresse IP non-grid, sauf si vous ajoutez l'adresse IP à la liste des adresses privilégiées. Vous pouvez uniquement fermer les ports ouverts par défaut et uniquement ouvrir les ports que vous avez fermés.



Les paramètres de l'onglet « Gérer l'accès externe » ne peuvent pas prévaloir sur ceux de l'onglet « Réseau client non fiable ». Par exemple, si un nœud est non fiable, le port SSH/22 est bloqué sur le réseau client, même s'il est ouvert dans l'onglet « Gérer l'accès externe ». Les paramètres de l'onglet « Réseau client non fiable » prévalent sur les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau répertoriant tous les ports externes (ports accessibles par défaut aux nœuds hors grille) des nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
 - Utilisez le bouton à bascule situé à côté de chaque port pour ouvrir ou fermer le port sélectionné.
 - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
 - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports listés dans le tableau.



Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.



Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous saisissez **2**, tous les ports dont le nom contient la chaîne « 2 » seront affichés.

3. Sélectionnez **Save**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud n'accepte le trafic entrant que sur les ports

configurés comme points de terminaison d'équilibrage de charge et, éventuellement, sur les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour définir le paramètre par défaut des nouveaux nœuds ajoutés lors d'une extension.



Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration que vous effectuez dans l'onglet **Réseau client non approuvé** remplacent les paramètres de l'onglet **Gérer l'accès externe**.

Étapes

1. Sélectionnez **Réseau client non approuvé**.
2. Dans la section Définir la valeur par défaut des nouveaux nœuds, spécifiez le paramètre par défaut qui doit être appliqué lorsque de nouveaux nœuds sont ajoutés à la grille lors d'une procédure d'expansion.
 - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est fiable.
 - **Non fiable** : Lorsqu'un nœud est ajouté lors d'une extension, son réseau client est non fiable.

Au besoin, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.



Ce paramètre n'affecte pas les nœuds existants de votre système StorageGRID.

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés ou sur des ports supplémentaires sélectionnés :
 - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste Untrusted Client Network.
 - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Untrusted Client Network.
 - Utilisez le bouton bascule situé à côté de chaque nœud pour définir le réseau client comme étant de confiance ou non de confiance pour le nœud sélectionné.

Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste Réseau client non fiable, puis utiliser le bouton bascule situé à côté d'un nœud individuel pour ajouter ce nœud à la liste Réseau client fiable.



Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous saisissez **GW**, tous les nœuds dont le nom contient la chaîne "GW" seront affichés.

4. Sélectionnez **Enregistrer**.

Les nouveaux paramètres du pare-feu sont immédiatement appliqués et appliqués. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

Comptes locataires dans StorageGRID

Un compte locataire vous permet d'utiliser l'API REST du Simple Storage Service (S3) pour stocker et récupérer des objets dans un système StorageGRID.



Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Gérer les locataires"](#).

En tant qu'administrateur de grille, vous créez et gérez les comptes locataires que les clients S3 utilisent pour stocker et récupérer des objets.

Chaque compte locataire possède des groupes fédérés ou locaux, des utilisateurs, des compartiments S3 et des objets.

Les comptes locataires permettent de segmenter les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés dans les deux cas suivants :

- **Cas d'utilisation en entreprise** : Si vous administrez un système StorageGRID dans une application d'entreprise, vous pouvez vouloir segmenter le stockage d'objets de la grille en fonction des différents services de votre organisation. Dans ce cas, vous pouvez créer des comptes locataires pour le service Marketing, le service Support Client, le service Ressources Humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez utiliser les compartiments S3 et les stratégies de compartiment pour segmenter les objets entre les services d'une entreprise. Vous n'avez pas besoin d'utiliser des comptes locataires. Consultez les instructions pour implémenter ["Compartiments S3 et politiques de compartiment"](#) pour plus d'informations.

- **Cas d'utilisation pour un fournisseur de services** : Si vous administrez un système StorageGRID en tant que fournisseur de services, vous pouvez segmenter le stockage d'objets de la grille en fonction des différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes clients pour Company A, Company B, Company C, etc.

Pour plus d'informations, consultez ["Utilisez un compte locataire"](#).

Comment créer un compte locataire ?

Utilisez le gestionnaire Grid pour créer un compte locataire. Lorsque vous créez un compte locataire, vous spécifiez les informations suivantes :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Les autorisations du compte locataire, telles que la possibilité pour ce dernier d'utiliser les services de la plateforme S3, de configurer sa propre source d'identité, d'utiliser S3 Select ou d'utiliser une connexion de fédération de grille.
- L'accès racine initial du locataire, en fonction de la manière dont le système StorageGRID utilise les groupes et utilisateurs locaux, la fédération d'identités ou l'authentification unique (SSO).

De plus, vous pouvez activer le paramètre S3 Object Lock pour le système StorageGRID si les comptes locataires S3 doivent se conformer aux exigences réglementaires. Lorsque S3 Object Lock est activé, tous les comptes locataires S3 peuvent créer et gérer des compartiments conformes.

À quoi sert Tenant Manager ?

Une fois le compte locataire créé, les utilisateurs locataires peuvent se connecter au Gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

- Configurer la fédération d'identités (sauf si la source d'identité est partagée avec la grille)
- Gérer les groupes et les utilisateurs
- Utilisez la fédération de grilles pour le clonage de comptes et la réplication inter-grilles
- Gérer les clés d'accès S3
- Créer et gérer des compartiments S3
- Utilisez les services de la plateforme S3
- Utilisez S3 Select
- Surveiller l'utilisation du stockage



Bien que les utilisateurs d'un locataire S3 puissent créer et gérer des clés d'accès S3 et des compartiments avec le Tenant Manager, ils doivent utiliser une application cliente S3 pour ingérer et gérer les objets. Voir ["Utilisez l'API REST S3"](#) pour plus de détails.

Créer un compte locataire StorageGRID

Vous devez créer au moins un compte locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Les étapes de création d'un compte locataire varient selon que ["fédération d'identité"](#) et ["authentification unique"](#) sont configurés et selon que le compte Grid Manager que vous utilisez pour créer le compte locataire appartient à un groupe d'administrateurs disposant de l'autorisation d'accès Root.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root ou autorisation de comptes locataires"](#).
- Si le compte locataire utilise la source d'identité configurée pour le Grid Manager et que vous souhaitez accorder l'autorisation d'accès Root à un groupe fédéré pour ce compte, vous avez importé ce groupe fédéré dans le Grid Manager. Vous n'avez pas besoin d'attribuer d'autorisations Grid Manager à ce groupe d'administrateurs. Voir ["Gérer les groupes d'administrateurs"](#).
- Si vous souhaitez autoriser un locataire S3 à cloner les données d'un compte et à répliquer les objets d'un compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles :
 - Vous avez ["configuré la connexion de fédération de grille"](#).
 - L'état de la connexion est **Connecté**.
 - Vous disposez des droits d'accès root.
 - Vous avez examiné les éléments à prendre en compte pour ["gestion des locataires autorisés pour la fédération de grid"](#).
 - Si le compte locataire utilisera la source d'identité qui a été configurée pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

Lors de la création du locataire, vous sélectionnez ce groupe pour avoir l'autorisation d'accès Root initiale pour les comptes de locataire source et de destination.



Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant que vous ne créiez le locataire, le locataire n'est pas répliqué vers la destination.

Accédez à l'assistant

Étapes

1. Sélectionnez **Tenants**.
2. Sélectionnez **Create**.

Saisissez les détails

Étapes

1. Saisissez les informations concernant le locataire.

Champ	Description
Nom	Nom du compte locataire. Les noms de locataire n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un identifiant de compte unique à 20 chiffres.
Description (facultatif)	Une description permettant d'identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grilles, vous pouvez éventuellement utiliser ce champ pour vous aider à identifier lequel est le locataire source et lequel est le locataire de destination. Par exemple, cette description pour un locataire créé sur Grid 1 apparaîtra également pour le locataire répliqué sur Grid 2 : « Ce locataire a été créé sur Grid 1. »
Type de client	Doit être S3 .
Quota de stockage (facultatif)	Si vous souhaitez attribuer un quota de stockage à ce locataire, indiquez une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continue**.

Sélectionnez les autorisations

Étapes

1. Vous pouvez également sélectionner les autorisations de base que vous souhaitez que ce locataire ait.



Certaines de ces autorisations comportent des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisation	Si sélectionné...
Autoriser les services de plateforme	Le locataire peut utiliser les services de la plateforme S3 tels que CloudMirror. Voir " Gérer les services de plateforme pour les comptes locataires S3 ".

Autorisation	Si sélectionné...
Utiliser votre propre source d'identité	Le locataire peut configurer et gérer sa propre source d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous avez "SSO configuré" pour votre système StorageGRID.
Autoriser S3 Select	Le locataire peut émettre des requêtes API S3 SelectObjectContent pour filtrer et récupérer les données d'objet. Voir "Gérer S3 Select pour les comptes locataires". Important : les requêtes SelectObjectContent peuvent dégrader les performances de l'équilibreur de charge pour tous les clients et locataires S3. N'activez cette fonctionnalité qu'en cas de besoin et uniquement pour les locataires de confiance.

2. Vous pouvez également sélectionner les autorisations avancées que vous souhaitez que ce locataire possède.

Autorisation	Si sélectionné...
Connexion de fédération de grille	Le locataire peut utiliser une connexion de fédération de grille, qui : - Fait en sorte que ce locataire, ainsi que tous les groupes de locataires et les utilisateurs ajoutés au compte, soient clonés à partir de cette grille (la <i>grille source</i>) vers l'autre grille de la connexion sélectionnée (la <i>grille de destination</i>). - Permet à ce locataire de configurer la réplication inter-grilles entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération de grid".
Verrouillage d'objet S3	Autorisez le locataire à utiliser certaines fonctionnalités de S3 Object Lock : Définir la période de rétention maximale définit la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. Autoriser le mode de conformité empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégés pendant la période de conservation.

3. Sélectionnez **Continue**.

Définissez l'accès root et créez un locataire

Étapes

- Définissez l'accès racine pour le compte locataire, selon que votre système StorageGRID utilise la fédération d'identités, l'authentification unique (SSO) ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir l'autorisation d'accès Root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant auquel vous accordez l'autorisation d'accès Root pour le locataire. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer un locataire**.

Un message de confirmation s'affiche et le nouveau locataire est répertorié sur la page Locataires. Pour savoir comment consulter les détails d'un locataire et suivre son activité, voir ["Surveiller l'activité des locataires"](#).



L'application des paramètres locataires à l'ensemble de la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état des nœuds et des opérations Cassandra.

3. Si vous avez sélectionné l'autorisation **Utiliser la connexion de fédération de grille** pour le locataire :

- Vérifiez qu'un locataire identique a bien été répliqué sur l'autre grille de la connexion. Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations.



Si vous voyez le message d'erreur « Tenant created without a clone », reportez-vous aux instructions dans ["Dépanner les erreurs de fédération de grille"](#).

- Si vous avez fourni un mot de passe d'utilisateur root local lors de la définition de l'accès root, ["modifier le mot de passe de l'utilisateur root local"](#) pour le locataire répliqué.



Un utilisateur racine local ne peut pas se connecter à Tenant Manager sur la grille de destination tant que le mot de passe n'est pas modifié.

Se connecter au locataire (facultatif)

Selon vos besoins, vous pouvez vous connecter dès maintenant au nouveau tenant pour terminer la configuration, ou vous pouvez vous connecter au tenant ultérieurement. Les étapes de connexion dépendent du fait que vous êtes connecté à Grid Manager en utilisant le port par défaut (443) ou un port restreint. Voir ["Contrôler l'accès au niveau du pare-feu externe"](#).

Connectez-vous maintenant

Si vous utilisez...	Faites ceci...
Le port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez Se connecter en tant que root. Lorsque vous vous connectez, des liens apparaissent pour configurer les compartiments, la fédération d'identités, les groupes et les utilisateurs. 2. Sélectionnez les liens pour configurer le compte tenant. Chaque lien ouvre la page correspondante dans le Tenant Manager. Pour compléter la page, consultez le "instructions pour l'utilisation des comptes locataires".
Le port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez Se connecter , puis saisissez les informations d'identification d'un utilisateur du groupe fédéré d'accès racine.
Un port restreint	1. Sélectionnez Terminer 2. Sélectionnez Restreint dans le tableau Tenant pour en savoir plus sur l'accès à ce compte locataire. L'URL du Tenant Manager a le format suivant : <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</code> ° <i>FQDN_or_Admin_Node_IP</i> est un 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'identifiant unique du compte du locataire

Se connecter plus tard

Si vous utilisez...	Effectuez l'une de ces actions...
Port 443	• Dans le Grid Manager, sélectionnez Tenants, puis Sign in à droite du nom du tenant. • Saisissez l'URL du locataire dans un navigateur Web : <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code> ° <i>FQDN_or_Admin_Node_IP</i> est un domaine complet ou l'adresse IP d'un nœud d'administration ° <i>20-digit-account-id</i> est l'identifiant unique du compte du locataire

Si vous utilisez...	Effectuez l'une de ces actions...
Un port restreint	- Dans le Grid Manager, sélectionnez Tenants, puis Restricted. - Saisissez 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 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'identifiant unique du compte du locataire

Configurer le locataire

Suivez les instructions dans ["Utilisez un compte locataire"](#) pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les compartiments, les services de plateforme, ainsi que le clonage de compte et la réplication inter-grilles.

Modifier un compte locataire StorageGRID

Vous pouvez modifier un compte locataire pour changer le nom d'affichage, le quota de stockage ou les autorisations du locataire.



Si un locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vous pouvez modifier les informations du locataire depuis l'une ou l'autre des grilles de la connexion. Cependant, toute modification effectuée sur une grille de la connexion ne sera pas copiée sur l'autre grille. Si vous souhaitez que les informations du locataire restent parfaitement synchronisées entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir ["Gérer les locataires autorisés pour la connexion à la fédération de grid"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root ou autorisation de comptes locataires"](#).



L'application des paramètres locataires à l'ensemble de la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état des nœuds et des opérations Cassandra.

Étapes

- Sélectionnez **Tenants**.

Tenants

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

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Localisez le compte locataire que vous souhaitez modifier.

Utilisez le champ de recherche pour rechercher un locataire par son nom ou son identifiant de locataire.

3. Sélectionnez le locataire. Vous pouvez procéder de l'une des manières suivantes :

- Sélectionnez la case à cocher du locataire, puis sélectionnez **Actions** > **Edit**.
- Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Modifier**.

4. Vous pouvez éventuellement modifier les valeurs de ces champs :

- **Nom**
- **Description**
- **Quota de stockage**

5. Sélectionnez **Continue**.

6. Sélectionnez ou désélectionnez les autorisations du compte locataire.

- Si vous désactivez les **Services de plateforme** pour un locataire qui les utilise déjà, les services qu'il a configurés pour ses compartiments S3 cesseront de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il pourra toujours stocker des objets dans le compartiment, mais des copies de ces objets ne seront plus créées dans le compartiment S3 externe qu'il a configuré comme point de terminaison. Voir ["Gérer les services de plateforme pour les comptes locataires S3"](#).
- Modifiez le paramètre **Utiliser sa propre source d'identité** pour déterminer si le compte locataire utilisera sa propre source d'identité ou la source d'identité configurée pour Grid Manager.

Si **Utiliser votre propre source d'identité** est :

- Désactivé et sélectionné, le locataire a déjà activé sa propre source d'identité. Un locataire doit désactiver sa source d'identité avant de pouvoir utiliser la source d'identité configurée pour le Grid Manager.
- Désactivé et non sélectionné, l'authentification unique (SSO) est activée pour le système StorageGRID. Le locataire doit utiliser la source d'identité qui a été configurée pour le Grid

Manager.

- Sélectionnez ou désactivez l'autorisation **Allow S3 Select** selon vos besoins. Voir "[Gérer S3 Select pour les comptes locataires](#)".
- Pour supprimer l'autorisation **Utiliser la connexion de fédération de grille** :
 - i. Sélectionnez l'onglet **Fédération de grilles**.
 - ii. Sélectionnez **Supprimer l'autorisation**.
- Pour ajouter l'autorisation **Utiliser la connexion de fédération de grille** :
 - i. Sélectionnez l'onglet **Fédération de grilles**.
 - ii. Cochez la case **Utiliser la connexion de fédération de grille**.
 - iii. Vous pouvez également sélectionner **Cloner les utilisateurs et groupes locaux existants** pour les cloner sur la grille distante. Si vous le souhaitez, vous pouvez interrompre le clonage en cours ou réessayer de cloner si certains utilisateurs ou groupes locaux n'ont pas pu être clonés après la dernière opération de clonage.
- Pour définir une durée de conservation maximale ou autoriser le mode de conformité :



Le verrouillage d'objet S3 doit être activé sur la grille avant que vous puissiez utiliser ces paramètres.

- i. Sélectionnez l'onglet **Verrouillage d'objet S3**.
- ii. Pour **Définir la période de conservation maximale**, saisissez une valeur et sélectionnez la période dans le menu déroulant.
- iii. Pour **Allow compliance mode**, cochez la case.

Modifier le mot de passe de l'utilisateur root local d'un locataire StorageGRID

Vous devrez peut-être modifier le mot de passe de l'utilisateur racine local d'un locataire si l'utilisateur racine est verrouillé hors de son compte.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

À propos de cette tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte du locataire. Pour effectuer des tâches d'utilisateur root, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès Root pour le locataire.

Étapes

1. Sélectionnez **Tenants**.

Tenants

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

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

- Sélectionnez le compte locataire. Vous pouvez effectuer l'une des actions suivantes :
 - Sélectionnez la case à cocher correspondant au locataire, puis sélectionnez **Actions** > **Modifier le mot de passe racine**.
 - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions** > **Changer le mot de passe racine**.
- Saisissez le nouveau mot de passe du compte locataire.
- Sélectionnez **Enregistrer**.

Supprimer un compte locataire StorageGRID

Vous pouvez supprimer un compte locataire si vous souhaitez supprimer définitivement l'accès du locataire au système.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez supprimé tous les compartiments S3 et les objets associés au compte du locataire.
- Si le locataire est autorisé à utiliser une connexion de fédération de grille, vous avez examiné les considérations relatives à ["suppression d'un locataire disposant de l'autorisation « Utiliser la connexion de fédération de grille »"](#).

Étapes

- Sélectionnez **Tenants**.
- Localisez le ou les comptes locataires que vous souhaitez supprimer.

Utilisez le champ de recherche pour rechercher un locataire par son nom ou son identifiant de locataire.

- Pour supprimer plusieurs locataires, cochez les cases et sélectionnez **Actions** > **Supprimer**.
- Pour supprimer un seul locataire, procédez de l'une des manières suivantes :

- Cochez la case, puis sélectionnez **Actions > Supprimer**.
- Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions > Delete**.

5. Sélectionnez **Oui**.

Gérer les services de plateforme

Découvrez les services de la plateforme StorageGRID

Les services de la plateforme incluent la réplication CloudMirror, les notifications d'événements et le service d'intégration de recherche.

Si vous activez les services de plateforme pour les comptes locataires S3, vous devez configurer votre grille afin que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Les services de plateforme ne sont pas pris en charge pour ["seaux de branches"](#).

Réplication CloudMirror

Le service de réplication CloudMirror StorageGRID est utilisé pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grilles. Pour en savoir plus, consultez ["Comparez la réplication inter-grilles et la réplication CloudMirror"](#).



CloudMirror replication n'est pas prise en charge si le compartiment source a le verrouillage d'objet S3 activé.

Notifications

Les notifications d'événements par compartiment sont utilisées pour envoyer des notifications concernant des actions spécifiques effectuées sur des objets à un cluster Kafka externe spécifié, à un point de terminaison webhook ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes pour qu'elles soient envoyées aux administrateurs concernant chaque objet ajouté à un compartiment, où les objets représentent des fichiers journaux associés à un événement système critique.



Bien que la notification d'événements puisse être configurée sur un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris Retain Until Date et Legal Hold status) 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 les métadonnées d'objets S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

Par exemple, vous pouvez configurer vos compartiments pour envoyer les métadonnées des objets S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans

vos compartiments et réaliser des analyses sophistiquées des tendances présentes dans les métadonnées de vos objets.



Bien que l'intégration d'Elasticsearch puisse être configurée sur un compartiment avec le S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation et le statut de Legal Hold) 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 est généralement externe à votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Si tel est le cas, vous devez activer l'utilisation des services de plateforme lors de la création ou de la modification des comptes locataires. Vous devez également configurer votre réseau afin que les messages des services de plateforme générés par les locataires puissent atteindre leurs destinations.

Recommandations pour l'utilisation des services de la plateforme

Avant d'utiliser les services de la plateforme, veuillez prendre connaissance des recommandations suivantes :

- Si un compartiment S3 dans le système StorageGRID a à la fois le versionnage et la réplication CloudMirror activés, vous devez également activer le versionnage du compartiment S3 pour le point de terminaison de destination. Cela permet à la réplication CloudMirror de générer des versions d'objets similaires sur le point de terminaison.
- Il est déconseillé d'utiliser plus de 100 locataires actifs pour les requêtes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration à la recherche. Un nombre supérieur à 100 locataires actifs peut entraîner une baisse des performances du client S3.
- Les requêtes vers un point de terminaison qui ne peuvent être traitées seront mises en file d'attente, dans la limite de 500 000 requêtes. Cette limite est répartie équitablement entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500 000 afin que les locataires nouvellement créés ne soient pas injustement pénalisés.

Informations connexes

- ["Gérer les services de plateforme"](#)
- ["Configurer les paramètres du proxy de stockage"](#)
- ["Surveiller StorageGRID"](#)

Réseau et ports pour les services de plateforme StorageGRID

Si vous autorisez un locataire S3 à utiliser les services de plateforme, vous devez configurer le réseau pour la grille afin de garantir que les messages des services de plateforme puissent être livrés à leurs destinations.

Vous pouvez activer les services de plateforme pour un compte locataire S3 lors de la création ou de la mise à jour du compte locataire. Si les services de plateforme sont activés, le locataire peut créer des points de terminaison servant de destination pour la réplication CloudMirror, les notifications d'événements ou les messages d'intégration de recherche provenant de ses compartiments S3. Ces messages de services de plateforme sont envoyés des nœuds de stockage exécutant le service ADC vers les points de terminaison de destination.

Par exemple, les locataires peuvent configurer les types de points de terminaison de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Une application locale qui prend en charge la réception des messages Amazon Simple Notification Service
- Un cluster Kafka hébergé localement
- Un point de terminaison webhook externe ou hébergé localement qui prend en charge les requêtes de notification HTTP POST.

Ce point de terminaison peut être hébergé sur divers serveurs web, frameworks ou outils de traitement des données tels que Fluentd.

- Un compartiment S3 hébergé localement sur la même instance ou une autre instance de StorageGRID
- Un point de terminaison externe, tel qu'un point de terminaison sur Amazon Web Services.

Pour garantir la transmission des messages des services de plateforme, vous devez configurer le ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer les messages des services de plateforme aux points de terminaison de destination.

Par défaut, les messages des services de la plateforme sont envoyés sur les ports suivants :

- **80** : Pour les URI de point de terminaison qui commencent par http (la plupart des points de terminaison)
- **443** : Pour les URI de points de terminaison qui commencent par https (la plupart des points de terminaison)
- **9092** : Pour les URI d'endpoint qui commencent par http ou https (endpoints Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un point de terminaison.



Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, les messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Assurez-vous que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le point de terminaison.

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

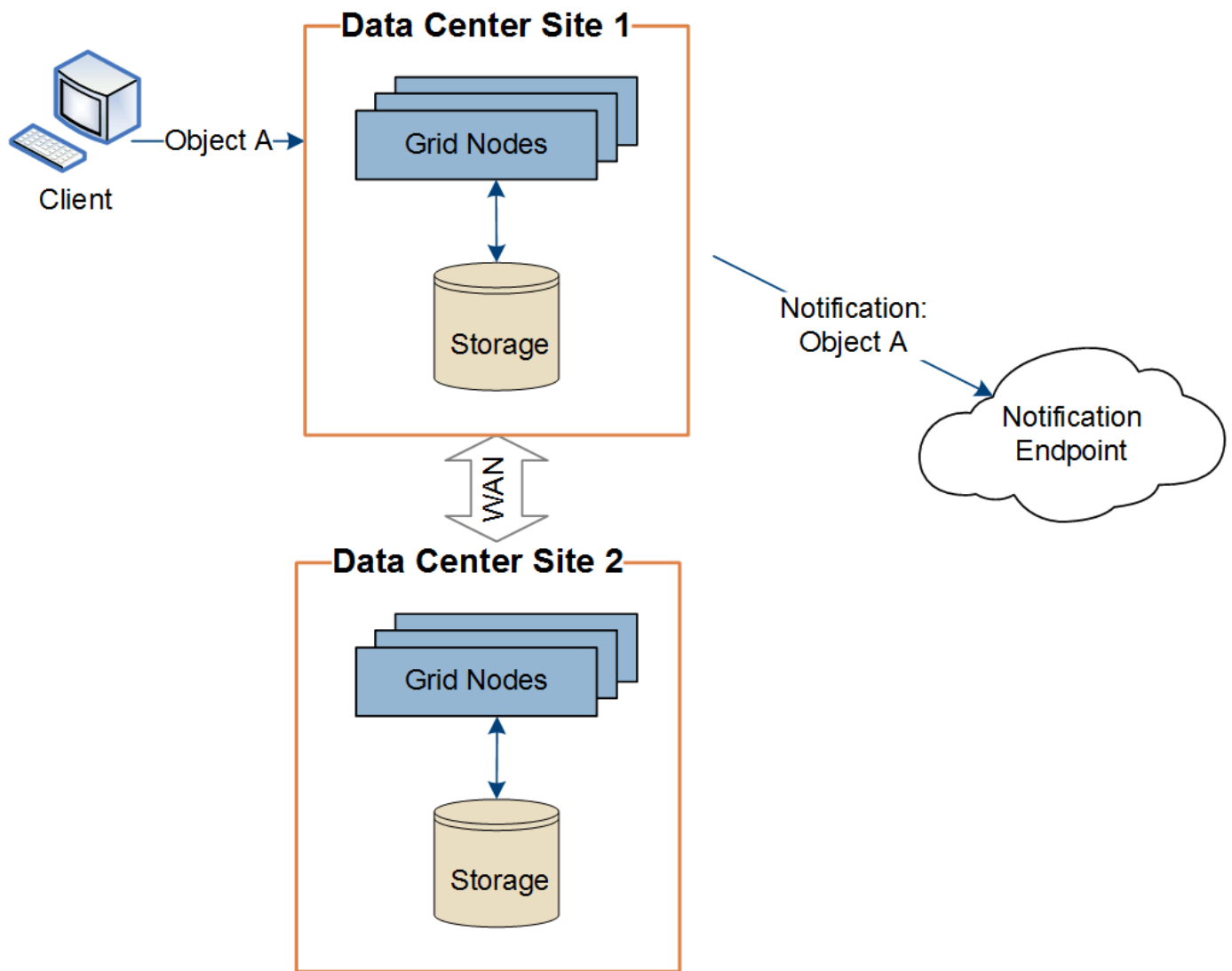
Informations connexes

["Utilisez un compte locataire"](#)

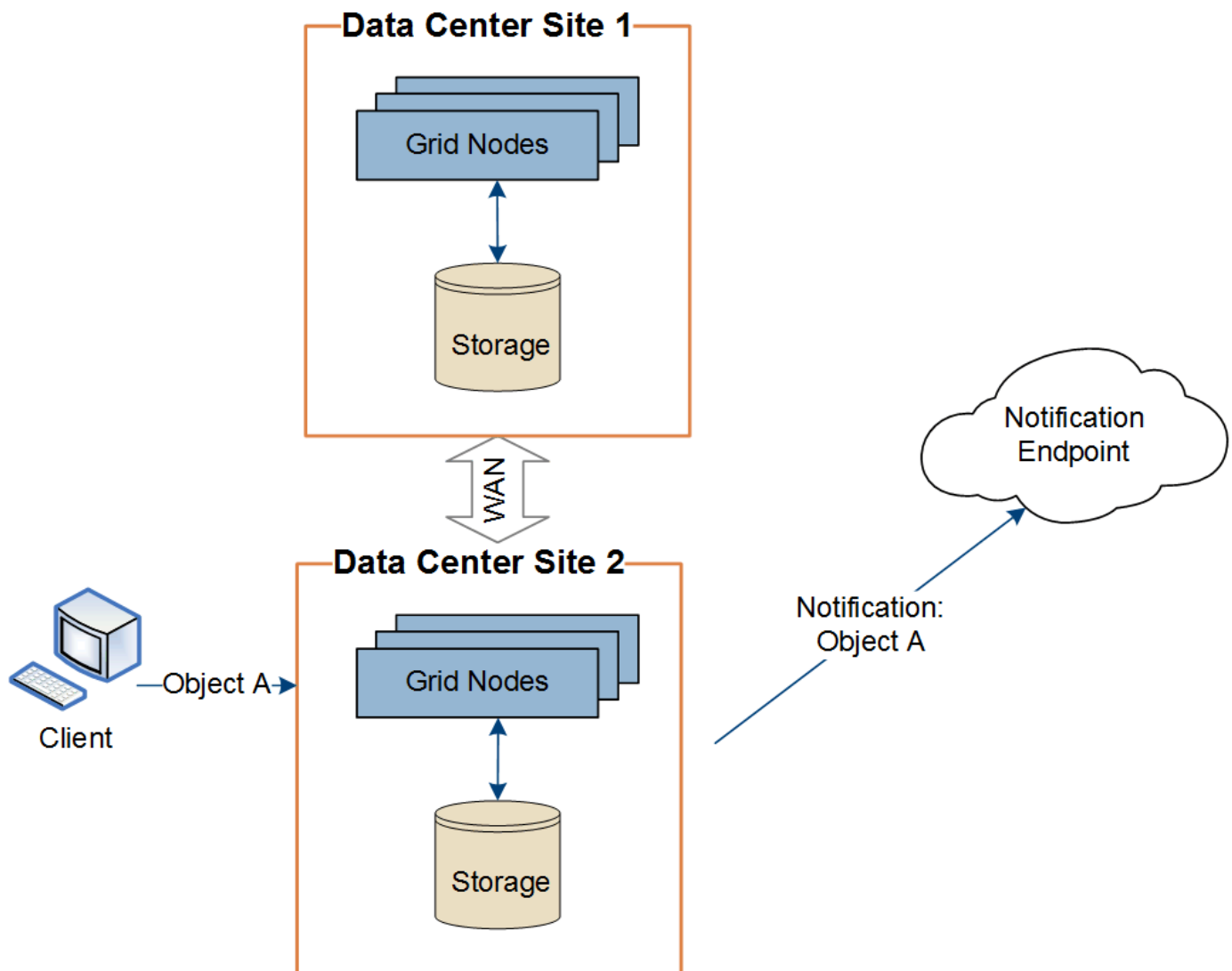
Livraison par site des messages des services de plateforme StorageGRID

Toutes les opérations des services de la plateforme sont effectuées site par site.

Autrement dit, si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle du Data Center Site 1, la notification concernant cette action est déclenchée et envoyée depuis le Data Center Site 1.



Si le client effectue ultérieurement une opération Delete de l'API S3 sur ce même objet depuis Data Center Site 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis Data Center Site 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de la plateforme puissent être acheminés vers leurs destinations.

Dépanner les services de plateforme StorageGRID

Les points de terminaison utilisés dans les services de la plateforme sont créés et gérés par les utilisateurs locataires dans le Tenant Manager. Cependant, si un locataire rencontre des difficultés pour configurer ou utiliser les services de la plateforme, vous pouvez utiliser le Grid Manager pour aider à résoudre le problème.

Problèmes liés aux nouveaux points de terminaison

Avant qu'un locataire puisse utiliser les services de la plateforme, il doit créer un ou plusieurs points de terminaison à l'aide du Tenant Manager. Chaque point de terminaison représente une destination externe pour un service de la plateforme, telle qu'un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet Amazon Simple Notification Service, un sujet Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque point de terminaison inclut à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un point de terminaison, le système StorageGRID vérifie que le point de terminaison existe et qu'il est accessible à l'aide des identifiants spécifiés. La connexion au point de terminaison est

validée à partir d'un nœud sur chaque site.

En cas d'échec de la validation du point de terminaison, un message d'erreur explique la raison de cet échec. L'utilisateur du locataire doit résoudre le problème, puis essayer de créer à nouveau le point de terminaison.



La création du point de terminaison échouera si les services de la plateforme ne sont pas activés pour le compte du locataire.

Problèmes liés aux points de terminaison existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un point de terminaison existant, un message s'affiche sur le tableau de bord du Tenant Manager.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Les utilisateurs locataires peuvent accéder à la page « Points de terminaison » pour examiner le message d'erreur le plus récent pour chaque point de terminaison et déterminer depuis combien de temps l'erreur s'est produite. La colonne « Dernière erreur » affiche le message d'erreur le plus récent pour chaque point de terminaison et indique depuis combien de temps l'erreur s'est produite. Les erreurs qui incluent l'icône  se sont produites au cours des 7 derniers jours.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

☐	Display name 	Last error 	Type 	URI 	URN 
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Certains messages d'erreur de la colonne **Dernière erreur** peuvent contenir un logID entre parenthèses. Un administrateur de grille ou le support technique peut utiliser ce logID pour trouver des informations plus détaillées sur l'erreur dans le fichier bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un "proxy de stockage" entre les nœuds de stockage et les points de terminaison des services de la plateforme, des erreurs peuvent survenir si votre service proxy n'autorise pas les messages provenant de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy afin de vous assurer que les messages relatifs aux services de la plateforme ne sont pas bloqués.

Déterminez si une erreur s'est produite

Si des erreurs de point de terminaison se sont produites au cours des 7 derniers jours, le tableau de bord du Tenant Manager affiche un message d'alerte. Vous pouvez accéder à la page Endpoints pour voir plus de détails sur l'erreur.

Les opérations du client échouent

Certains problèmes liés aux services de la plateforme peuvent entraîner l'échec des opérations client sur le compartiment S3. Par exemple, les opérations client S3 échoueront si le service interne Replicated State Machine (RSM) s'arrête ou si un trop grand nombre de messages de services de plateforme sont en attente de livraison.

Pour vérifier l'état des services :

1. Sélectionnez **Nodes > site > Storage Node > Overview**.
2. Vérifiez les alertes actives dans le tableau des alertes.
3. Résolvez les alertes en cours. Au besoin, contactez le support technique.

Erreurs de point de terminaison récupérables et irrécupérables

Une fois les points de terminaison créés, des erreurs de requête de service de la plateforme peuvent survenir pour diverses raisons. Certaines erreurs sont récupérables avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent survenir pour les raisons suivantes :

- Les identifiants de l'utilisateur ont été supprimés ou ont expiré.
- Le compartiment de destination n'existe pas.
- La notification ne peut pas être transmise.

Si StorageGRID rencontre une erreur récupérable, la requête de service de la plateforme sera réessayée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, des erreurs irrécupérables peuvent survenir pour les raisons suivantes :

- Le point de terminaison a été supprimé.
- Un point de terminaison webhook de destination répond à une requête de notification par une erreur 400 `Bad Request`.

Si StorageGRID rencontre une erreur de point de terminaison irrécupérable :

- Dans le Gestionnaire de grille, accédez à **Support > Outils > Métriques > Grafana > Platform Services Overview** pour afficher les détails de l'erreur.
- Dans le Gestionnaire de locataires, accédez à **STOCKAGE (S3) > Points de terminaison des services de plateforme** pour afficher les détails de l'erreur.

- Vérifiez la `/var/local/log/bycast-err.log` pour les erreurs associées. Les nœuds de stockage disposant du service ADC contiennent ce fichier journal.

Les messages des services de la plateforme ne peuvent pas être remis.

Si la destination rencontre un problème l'empêchant de recevoir les messages des services de plateforme, l'opération client sur le compartiment réussit, mais le message des services de plateforme n'est pas transmis. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination et que StorageGRID ne peut plus s'authentifier auprès du service de destination.

Vérifiez les alertes associées.

Performances ralenties pour les requêtes de service de la plateforme

Le logiciel StorageGRID peut limiter le nombre de requêtes S3 entrantes pour un compartiment si le débit d'envoi des requêtes dépasse le débit auquel le point de terminaison de destination peut les recevoir. La limitation ne se produit que lorsqu'il y a un retard d'envoi des requêtes en attente vers le point de terminaison de destination.

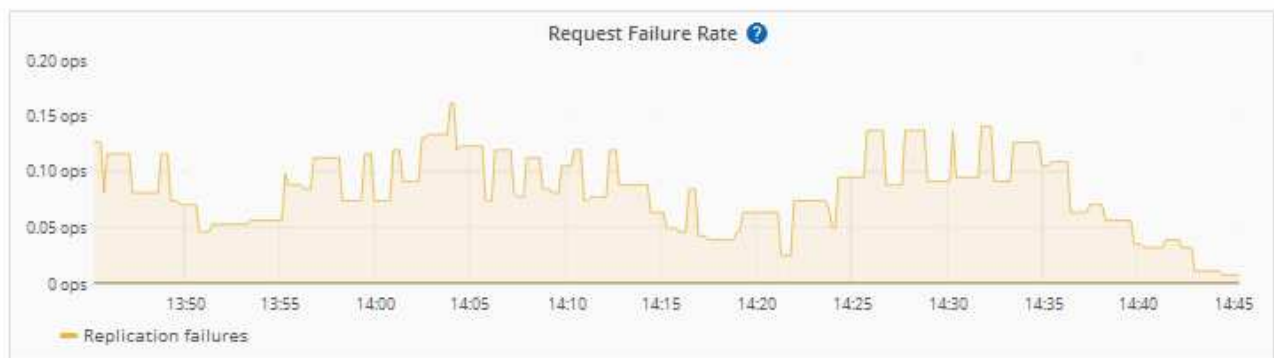
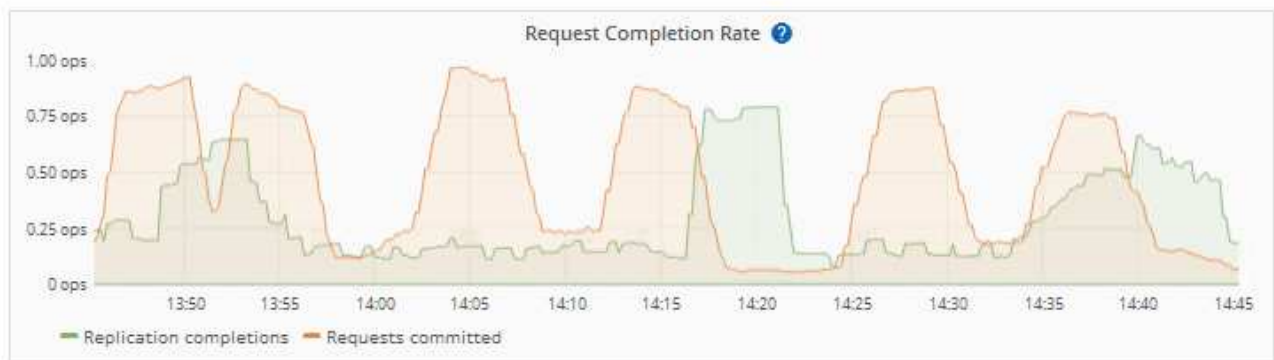
Le seul effet visible est un allongement du temps d'exécution des requêtes S3 entrantes. Si vous constatez un ralentissement significatif des performances, vous devez réduire le débit d'ingestion ou utiliser un point de terminaison offrant une capacité supérieure. Si le nombre de requêtes en attente continue d'augmenter, les opérations S3 côté client (telles que les requêtes PUT) finiront par échouer.

CloudMirror Les requêtes sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car elles impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

Les requêtes de service de la plateforme échouent

Pour consulter le taux d'échec des requêtes pour les services de la plateforme :

1. Sélectionnez **Nœuds**.
2. Sélectionnez **site** > **Services de plateforme**.
3. Consultez le graphique du taux d'erreur des requêtes.

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

Alerte d'indisponibilité des services de la plateforme

L'alerte **Services de plateforme indisponibles** indique qu'aucune opération de service de plateforme ne peut être effectuée sur un site, car trop peu de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles.

Le service RSM garantit que les requêtes de service de la plateforme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, identifiez les nœuds de stockage du site qui hébergent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui hébergent également le service ADC.) Ensuite, assurez-vous qu'une majorité simple de ces nœuds de stockage sont en cours d'exécution et disponibles.



Si plusieurs nœuds de stockage contenant le service RSM tombent en panne sur un site, vous perdez toutes les requêtes de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les points de terminaison des services de plateforme

Pour plus d'informations, voir [Utiliser un compte locataire](#) > [Dépanner les points de terminaison des services de la plateforme](#).

Informations connexes

["Dépanner le système StorageGRID"](#)

Gérer S3 Select pour les comptes locataires dans StorageGRID

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des requêtes SelectObjectContent sur des objets individuels.

S3 Select offre une solution efficace pour effectuer des recherches dans de grands volumes de données sans nécessiter le déploiement d'une base de données et des ressources associées. Il permet également de réduire le coût et la latence de récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser des requêtes SelectObjectContent pour filtrer et récupérer uniquement les données nécessaires d'un objet. L'implémentation StorageGRID de S3 Select inclut un sous-ensemble des commandes et fonctionnalités de S3 Select.

Considérations et exigences relatives à l'utilisation de S3 Select

Exigences d'administration du grid

L'administrateur de la grille doit accorder aux locataires l'autorisation S3 Select. Sélectionnez **Autoriser S3 Select** lorsque ["création d'un locataire"](#) ou ["modification d'un locataire"](#).

Exigences relatives au format des objets

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets Parquet :
 - S3 Select prend uniquement en charge la compression par colonnes via GZIP ou Snappy. S3 Select ne prend pas en charge la compression de l'objet entier pour les objets Parquet.
 - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie comme CSV ou JSON.
 - La taille maximale d'un groupe de lignes non compressé est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
 - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.

Exigences relatives aux points de terminaison

La requête SelectObjectContent doit être envoyée à un ["Point de terminaison de l'équilibreur de charge"](#)

[StorageGRID](#)".

Les nœuds d'administration et de passerelle utilisés par le point de terminaison doivent être l'un des suivants :

- Un nœud d'appliance de services
- Un nœud logiciel basé sur VMware
- Un nœud bare metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.



SelectObjectContent requests peuvent dégrader les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. N'activez cette fonctionnalité qu'en cas de besoin et uniquement pour les locataires de confiance.

Voir la ["Instructions d'utilisation de S3 Select"](#).

Pour consulter ["Graphiques Grafana"](#) pour les opérations S3 Select au fil du temps, sélectionnez **Support > Outils > Métriques** dans le Grid Manager.

Configurer les connexions client

Configurer les connexions client S3 à StorageGRID

En tant qu'administrateur de grille, vous gérez les options de configuration qui contrôlent la manière dont les applications clientes S3 se connectent à votre système StorageGRID pour stocker et récupérer des données.



Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Configurez les connexions client S3 et Swift"](#).

Tâches de configuration

1. Effectuez les tâches préalables dans StorageGRID, en fonction de la manière dont l'application cliente se connectera à StorageGRID.

Tâches requises

Vous devez obtenir :

- adresses IP
- Noms de domaine
- certificat SSL

Tâches facultatives

Configurez éventuellement :

- Fédération d'identité
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez soit utiliser l'assistant de configuration S3, soit configurer chaque entité StorageGRID manuellement. +

Utilisez l'assistant de configuration S3

Suivez les étapes de l'assistant de configuration S3.

Configurer manuellement

1. Créer un groupe à haute disponibilité
2. Créer un point de terminaison d'équilibrage de charge
3. Créer un compte locataire
4. Créer un compartiment et des clés d'accès
5. Configurer la règle et la stratégie ILM

1. Utilisez l'application S3 pour établir la connexion à StorageGRID. Créez des entrées DNS pour associer les adresses IP aux noms de domaine que vous prévoyez d'utiliser.

Si nécessaire, effectuez une configuration supplémentaire de l'application.

2. Effectuez des tâches continues dans l'application et dans StorageGRID pour gérer et surveiller le stockage d'objets au fil du temps.

Informations nécessaires pour connecter StorageGRID à une application cliente

Avant de pouvoir connecter StorageGRID à une application cliente S3, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir certaines valeurs.

De quelles valeurs avez-vous besoin ?

Le tableau suivant présente les valeurs que vous devez configurer dans StorageGRID et indique où ces valeurs sont utilisées par l'application S3 et le serveur DNS.

Valeur	Où la valeur est configurée	Là où la valeur est utilisée
Adresses IP virtuelles (VIP)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	Application cliente
certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	Application cliente
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	• Application cliente • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > Locataire et compartiment	Application cliente
Nom du compartiment/conteneur	StorageGRID > Locataire et compartiment	Application cliente

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une ou l'autre des manières suivantes pour obtenir les informations nécessaires :

- Utilisez le **"Assistant de configuration S3"**. L'assistant de configuration S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser lors de la configuration de l'application S3. L'assistant vous guide à travers les étapes nécessaires et vous aide à garantir que vos paramètres respectent les bonnes pratiques de StorageGRID.



Si vous configurez une application S3, il est recommandé d'utiliser l'assistant de configuration S3, sauf si vous avez des exigences particulières ou si votre implémentation nécessite une personnalisation importante.

- Utilisez le **"FabricPool assistant de configuration"**. Similaire à l'assistant de configuration S3, l'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser lors de la configuration d'un niveau cloud FabricPool dans ONTAP.



Si vous prévoyez d'utiliser StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool, il est recommandé d'utiliser l'assistant de configuration FabricPool, sauf si vous savez que vous avez des exigences particulières ou si votre implémentation nécessite une personnalisation importante.

- **Configurez les éléments manuellement.** Si vous vous connectez à une application S3 et préférez ne pas utiliser l'assistant de configuration S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Procédez comme suit :
 - a. Configurez le groupe de haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir **"Configurer les groupes à haute disponibilité"**.

- b. Créez le point de terminaison de l'équilibreur de charge que l'application S3 utilisera. Voir ["Configurer les points de terminaison de l'équilibreur de charge"](#).
- c. Créez le compte locataire que l'application S3 utilisera. Voir ["Créer un compte locataire"](#).
- d. Pour un locataire S3, connectez-vous au compte du locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accédera à l'application. Voir ["Créez vos propres clés d'accès"](#).
- e. Créez un ou plusieurs compartiments S3 dans le compte du locataire. Pour S3, voir ["Créer un compartiment S3"](#).
- f. Pour ajouter des instructions de placement spécifiques aux objets appartenant au nouveau locataire ou compartiment/conteneur, créez une nouvelle règle ILM et activez une nouvelle stratégie ILM pour utiliser cette règle. Voir ["Créer une règle ILM"](#) et ["Créer une stratégie ILM"](#).

Sécurité des clients S3 dans StorageGRID

Les comptes locataires StorageGRID utilisent des applications clientes S3 pour enregistrer les données d'objets dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications clientes.

Résumé

La liste suivante résume la manière dont la sécurité est mise en œuvre pour l'API REST S3 :

Sécurité de la connexion

TLS

Authentification du serveur

Certificat serveur X.509 signé par l'autorité de certification système ou certificat serveur personnalisé fourni par l'administrateur

Authentification du client

ID de clé d'accès au compte S3 et clé d'accès secrète

Autorisation du client

Propriété du compartiment et toutes les politiques de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications clientes

Les applications clientes S3 peuvent se connecter au service d'équilibrage de charge sur les nœuds de passerelle ou les nœuds d'administration, ou directement aux nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, selon la façon dont vous ["configurer le point de terminaison de l'équilibreur de charge"](#).

Le protocole HTTPS assure une communication sécurisée et chiffrée (TLS) et est recommandé. Vous devez associer un certificat de sécurité au point de terminaison.

Le protocole HTTP offre une communication moins sécurisée et non chiffrée et ne devrait être utilisé que pour les environnements hors production ou de test.

- Les clients qui se connectent aux nœuds de stockage peuvent également utiliser HTTPS ou HTTP.

HTTPS est le protocole par défaut et est recommandé.

Le protocole HTTP offre une communication moins sécurisée et non chiffrée, mais peut être utilisé en option ["activé"](#) pour les environnements hors production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service d'équilibrage de charge et les nœuds de stockage au sein de la grille sont chiffrées, que le point de terminaison de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir ["en-têtes d'authentification HTTP"](#) à StorageGRID pour effectuer des opérations REST API.

Certificats de sécurité et applications clientes

Dans tous les cas, les applications clientes peuvent établir des connexions TLS en utilisant soit un certificat serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat généré par le système StorageGRID :

- Lorsque les applications clientes se connectent au service d'équilibrage de charge, elles utilisent le certificat configuré pour le point de terminaison de l'équilibreur de charge. Chaque point de terminaison d'équilibrage de charge possède son propre certificat—soit un certificat serveur personnalisé chargé par l'administrateur de la grille, soit un certificat généré par l'administrateur de la grille dans StorageGRID lors de la configuration du point de terminaison.

Voir ["Considérations relatives à l'équilibrage de charge"](#).

- Lorsque des applications clientes se connectent directement à un nœud de stockage, elles utilisent soit les certificats serveur générés par le système pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), soit un certificat serveur personnalisé unique fourni pour la grille par un administrateur de la grille. Voir ["ajoutez un certificat d'API S3 personnalisé"](#).

Les clients doivent être configurés pour faire confiance à l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de chiffrement pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS. Pour configurer les suites de chiffrement, accédez à **Configuration > Sécurité > Paramètres de sécurité** et sélectionnez **Stratégies TLS et SSH**.

Versions de TLS prises en charge

StorageGRID prend en charge TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utilisez l'assistant de configuration S3

Considérations et exigences de l'assistant de configuration StorageGRID S3

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID comme système de stockage d'objets pour une application S3.

Quand utiliser l'assistant de configuration S3

L'assistant de configuration S3 vous guide à chaque étape de la configuration de StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'utilisation de l'assistant, vous téléchargez des fichiers que vous pouvez utiliser pour saisir des valeurs dans l'application S3. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux meilleures pratiques StorageGRID.

Si vous disposez de l'["Autorisation d'accès root"](#), vous pouvez compléter l'assistant de configuration S3 lors de la première utilisation de StorageGRID Grid Manager, ou y accéder et le compléter ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement tout ou partie des éléments requis, puis utiliser l'assistant pour assembler les valeurs nécessaires à une application S3.

Avant d'utiliser l'assistant

Avant d'utiliser l'assistant, assurez-vous d'avoir rempli ces conditions préalables.

Obtenez des adresses IP et configurez des interfaces VLAN

Si vous configurez un groupe à haute disponibilité (HA), vous savez à quels nœuds l'application S3 se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le CIDR du sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel (VLAN) pour isoler le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#).

Configurer la fédération d'identité et l'authentification unique (SSO)

Si vous prévoyez d'utiliser la fédération d'identité ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès root pour le compte locataire que l'application S3 utilisera. Voir ["Utilisez la fédération d'identités"](#) et ["Configurer l'authentification unique"](#).

Obtenir et configurer les noms de domaine

Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées du serveur de noms de domaine (DNS) associeront ce FQDN aux adresses IP virtuelles (VIP) du groupe HA que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, vous devriez avoir ["noms de domaine de points de terminaison S3 configurés"](#). L'utilisation de requêtes de type hébergement virtuel est recommandée.

Passez en revue les exigences relatives à l'équilibreur de charge et au certificat de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID, vous avez pris connaissance des considérations générales relatives à l'équilibrage de charge. Vous disposez des certificats à importer ou des valeurs nécessaires à la génération d'un certificat.

Si vous prévoyez d'utiliser un point de terminaison d'équilibreur de charge externe (tiers), vous disposez du domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurez les connexions de fédération de grille

Si vous souhaitez autoriser le locataire S3 à cloner les données du compte et à répliquer les objets du compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles, confirmez les points suivants avant de démarrer l'assistant :

- Vous avez ["configuré la connexion de fédération de grille"](#).

- L'état de la connexion est **Connecté**.
- Vous disposez des droits d'accès root.

Accédez et complétez l'assistant de configuration S3 dans StorageGRID

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID afin de l'utiliser avec une application S3. L'assistant de configuration fournit les valeurs dont l'application a besoin pour accéder à un compartiment StorageGRID et y enregistrer des objets.

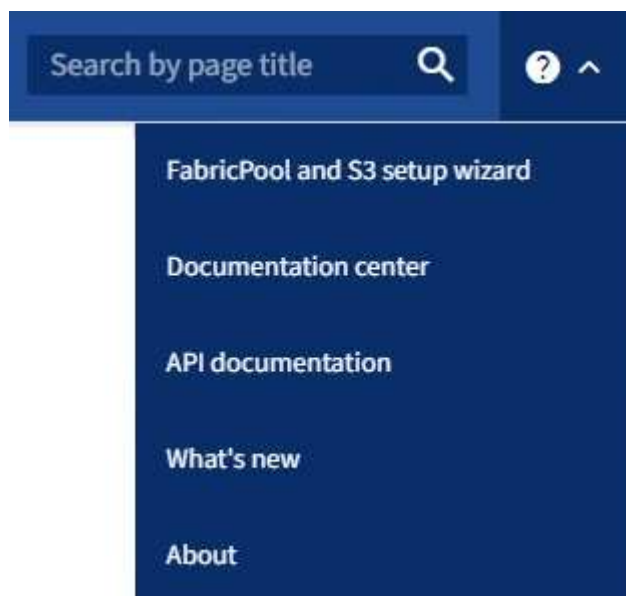
Avant de commencer

- Vous avez le "[Autorisation d'accès root](#)".
- Vous avez consulté les "[considérations et exigences](#)" instructions pour utiliser l'assistant.

Accédez à l'assistant

Étapes

1. Connectez-vous au Gestionnaire de grille en utilisant un "[navigateur Web pris en charge](#)".
2. Si la bannière **FabricPool and S3 setup wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du Grid Manager et sélectionnez **FabricPool and S3 setup wizard**.



3. Dans la section application S3 de la page de l'assistant de configuration FabricPool et S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 6 : Configurer le groupe HA

Un groupe HA est un ensemble de nœuds qui contiennent chacun le service d'équilibrage de charge StorageGRID. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe HA pour garantir la disponibilité des connexions de données S3. Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail avec peu

d'impact sur les opérations S3.

Pour plus de détails sur cette tâche, voir "[Gérer les groupes à haute disponibilité](#)".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez à [Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge](#).
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe HA ou utiliser un groupe HA existant.

Créer un groupe HA

- Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.
- Pour l'étape **Saisir les détails**, complétez les champs suivants.

Champ	Description
nom de groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

- À l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface par nœud.

- Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toute interface de secours pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs de la colonne **Ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active tombe en panne, les adresses IP virtuelles (VIP) sont transférées vers la première interface de secours par ordre de priorité. Si cette interface tombe en panne à son tour, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite. Une fois les pannes résolues, les adresses VIP sont réaffectées à l'interface prioritaire disponible.

- Pour l'étape **Saisir les adresses IP**, complétez les champs suivants.

Champ	Description
CIDR du sous-réseau	L'adresse du sous-réseau VIP en notation CIDR — une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit comporter aucun bit d'hôte activé. Par exemple, 192.16.0.0/22.
Adresse IP de la passerelle (facultatif)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP de StorageGRID, saisissez l'adresse IP de la passerelle locale VIP de StorageGRID. L'adresse IP de la passerelle locale doit appartenir au sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP. Au moins une adresse doit être de type IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

- f. Sélectionnez **Créer un groupe HA** puis **Terminer** pour revenir à l'assistant de configuration S3.
- g. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Utiliser le groupe HA existant

- a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans **Sélectionner un groupe HA**.
- b. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes. L'équilibrage de charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID, présent sur tous les nœuds Gateway et Admin, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, voir ["Considérations relatives à l'équilibrage de charge"](#).

Pour utiliser le service d'équilibrage de charge StorageGRID, sélectionnez l'onglet **StorageGRID load balancer**, puis créez ou sélectionnez le point de terminaison d'équilibrage de charge que vous souhaitez utiliser. Pour utiliser un équilibreur de charge externe, sélectionnez l'onglet **External load balancer** et fournissez les détails concernant le système que vous avez déjà configuré.

Créer un point de terminaison

Étapes

1. Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **Créer un point de terminaison**.
2. Pour l'étape **Saisir les détails du point de terminaison**, complétez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous saisissez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Remarque : Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir "Ports internes de StorageGRID".
Type de client	Doit être S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : La communication avec StorageGRID sans chiffrement TLS est prise en charge, mais n'est pas recommandée.

3. À l'étape **Sélectionnez le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le point de terminaison est accessible, soit via n'importe quelle adresse IP, soit via des adresses IP et des interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.

Mode	Description
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.

4. Pour l'étape d'accès du locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

5. Pour l'étape **Joindre le certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, la clé privée du certificat et, éventuellement, un ensemble de certificats d'autorité de certification.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Consultez " Configurer les points de terminaison de l'équilibreur de charge " pour plus de détails sur les informations à saisir.

Champ	Description
Utiliser le certificat StorageGRID S3	N'utilisez cette option que si vous avez déjà importé ou généré une version personnalisée du certificat global StorageGRID. Consultez " Configurer les certificats de l'API S3 " pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.

7. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.



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

Utilisez le point de terminaison de l'équilibreur de charge existant

Étapes

1. Pour utiliser un point de terminaison existant, sélectionnez son nom dans **Sélectionner un point de terminaison d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, complétez les champs suivants.

Champ	Description
FQDN	Le domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que l'application S3 utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

2. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Étape 3 sur 6 : Créez un locataire et un compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités.

Un bucket est un conteneur utilisé pour stocker les objets d'un locataire et les métadonnées des objets. Bien que les locataires puissent avoir plusieurs buckets, l'assistant vous aide à créer un locataire et un bucket de la manière la plus rapide et la plus simple. Si vous devez ajouter des buckets ou définir des options ultérieurement, vous pouvez utiliser le Tenant Manager.

Pour plus de détails sur cette tâche, consultez "[Créer un compte locataire](#)" et "[Créer un compartiment S3](#)".

Étapes

1. Saisissez un nom pour le compte locataire.

Les noms des locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un identifiant numérique unique.

2. Définissez l'accès racine pour le compte locataire, selon que votre système StorageGRID utilise "fédération d'identité", "authentification unique (SSO)" ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir "Autorisation d'accès root" pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour avoir "Autorisation d'accès root" pour le locataire. Aucun utilisateur local ne peut se connecter.

3. Si vous souhaitez que l'assistant crée l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur racine, sélectionnez **Créer automatiquement la clé d'accès S3 de l'utilisateur racine**.

Sélectionnez cette option si le seul utilisateur du locataire est l'utilisateur racine. Si d'autres utilisateurs utiliseront ce locataire, "utilisez Tenant Manager" pour configurer les clés et les autorisations.

4. Si vous souhaitez créer un compartiment pour ce locataire maintenant, sélectionnez **Créer un compartiment pour ce locataire**.



Si le S3 Object Lock est activé pour la grille, le compartiment créé à cette étape n'a pas le S3 Object Lock activé. Si vous devez utiliser un compartiment S3 Object Lock pour cette application S3, ne sélectionnez pas la création d'un compartiment maintenant. Utilisez plutôt Tenant Manager pour "créer le compartiment" ultérieurement.

a. Saisissez le nom du compartiment que l'application S3 utilisera. Par exemple, s3-bucket.

Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

b. Sélectionnez la **Région** pour ce compartiment.

Utilisez la région par défaut (us-east-1) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer**.

Étape 4 sur 6 : Télécharger les données

Lors de l'étape de téléchargement des données, vous pouvez télécharger un ou deux fichiers pour enregistrer les détails de ce que vous venez de configurer.

Étapes

1. Si vous avez sélectionné **Créer automatiquement une clé d'accès S3 pour l'utilisateur racine**, effectuez une ou les deux opérations suivantes :
 - Sélectionnez **Télécharger les clés d'accès** pour télécharger un `.csv` fichier contenant le nom du compte tenant, l'ID de la clé d'accès et la clé d'accès secrète.
 - Sélectionnez l'icône de copie () pour copier l'ID de clé d'accès et la clé d'accès secrète dans le presse-papiers.
2. Sélectionnez **Télécharger les valeurs de configuration** pour télécharger un `.txt` fichier contenant les paramètres du point de terminaison de l'équilibreur de charge, du tenant, du bucket et de l'utilisateur root.
3. Conservez ces informations dans un endroit sûr.



Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les clés ne seront plus disponibles après la fermeture de cette page. Veillez à conserver ces informations en lieu sûr, car elles peuvent être utilisées pour obtenir des données à partir de votre système StorageGRID.

4. Si le système vous y invite, cochez la case pour confirmer que vous avez téléchargé ou copié les clés.
5. Sélectionnez **Continuer** pour passer à l'étape relative à la règle et à la stratégie ILM.

Étape 5 sur 6 : Examiner la règle ILM et la politique ILM pour S3

Les règles de gestion du cycle de vie des informations (ILM) contrôlent l'emplacement, la durée de conservation et le comportement d'ingestion de tous les objets dans votre système StorageGRID. La stratégie ILM incluse avec StorageGRID crée deux copies répliquées de tous les objets. Cette stratégie reste en vigueur jusqu'à ce que vous activiez au moins une nouvelle stratégie.

Étapes

1. Examinez les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou compartiment, créez une nouvelle règle et une nouvelle stratégie. Voir "[Créer une règle ILM](#)" et "[Utilisez les politiques ILM](#)".
3. Sélectionnez **J'ai pris connaissance de ces étapes et je comprends ce que je dois faire**.
4. Cochez la case pour indiquer que vous comprenez ce que vous devez faire ensuite.
5. Sélectionnez **Continuer** pour accéder au **Résumé**.

Étape 6 sur 6 : Récapitulatif

Étapes

1. Consultez le résumé.
2. Prenez note des détails des étapes suivantes, qui décrivent la configuration supplémentaire pouvant être nécessaire avant de vous connecter au client S3. Par exemple, en sélectionnant **Se connecter en tant que root**, vous accédez au Tenant Manager, où vous pouvez ajouter des utilisateurs de locataire, créer des compartiments supplémentaires et mettre à jour les paramètres des compartiments.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier que vous avez téléchargé depuis StorageGRID ou des valeurs que vous avez obtenues manuellement.

Gérer les groupes HA

Découvrez les groupes de haute disponibilité StorageGRID

Les groupes à haute disponibilité (HA) fournissent des connexions de données à haute disponibilité pour les clients S3 et des connexions à haute disponibilité au Grid Manager et au Tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds Admin et Gateway dans un groupe à haute disponibilité (HA). Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail.

Chaque groupe HA donne accès aux services partagés sur les nœuds sélectionnés.

- Les groupes HA qui incluent des nœuds de passerelle, des nœuds d'administration ou les deux fournissent des connexions de données hautement disponibles pour les clients S3.
- Les groupes HA qui incluent uniquement des nœuds d'administration offrent des connexions à haute disponibilité au Grid Manager et au Tenant Manager.
- Un groupe HA composé uniquement d'appliances de services et de nœuds logiciels basés sur VMware peut fournir des connexions à haute disponibilité pour "[Les locataires S3 qui utilisent S3 Select](#)". Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais ne sont pas obligatoires.

Comment créer un groupe HA ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou nœuds de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface Client Network (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.



Vous ne pouvez pas ajouter une interface à un groupe HA si elle possède une adresse IP attribuée par DHCP.

2. Vous désignez une interface comme interface principale. L'interface principale est l'interface active sauf en cas de panne.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous attribuez de une à dix adresses IP virtuelles (VIP) au groupe. Les applications clientes peuvent utiliser n'importe laquelle de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, consultez "[Configurer les groupes à haute disponibilité](#)".

Qu'est-ce que l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe HA sont ajoutées à l'interface principale, qui est la première interface par ordre de priorité. Tant que l'interface principale reste disponible, elle est utilisée lorsque des clients se connectent à une adresse VIP du groupe. Autrement dit, en fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, en fonctionnement normal, les interfaces de priorité inférieure du groupe HA servent d'interfaces de secours. Ces interfaces de secours ne sont utilisées que si l'interface principale (actuellement active) devient indisponible.

Afficher l'état actuel du groupe HA d'un nœud

Pour voir si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **Nodes > node**.

Si l'onglet **Aperçu** comporte une entrée pour les **groupes HA**, le nœud est affecté aux groupes HA listés. La valeur après le nom du groupe correspond à l'état actuel du nœud dans le groupe HA :

- **Actif** : Le groupe HA est actuellement hébergé sur ce nœud.
- **Sauvegarde** : Le groupe HA n'utilise pas actuellement ce nœud ; il s'agit d'une interface de sauvegarde.
- **Arrêté** : Le groupe HA ne peut pas être hébergé sur ce nœud car le service de haute disponibilité (keepalived) a été arrêté manuellement.
- **Erreur** : Le groupe HA ne peut pas être hébergé sur ce nœud en raison d'un ou de plusieurs des éléments suivants :
 - Le service Load Balancer (nginx-gw) n'est pas en cours d'exécution sur le nœud.
 - L'interface eth0 ou VIP du nœud est hors service.
 - Le nœud est hors service.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active pour le groupe des clients d'administration et une interface de secours pour le groupe des 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 HA comprend plus d'une interface et que l'interface active tombe en panne, les adresses VIP sont transférées vers la première interface de secours disponible selon l'ordre de priorité. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée tombe en panne.
- Le nœud sur lequel l'interface est configurée perd la connectivité avec tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service d'équilibrage de charge s'arrête.
- Le service de haute disponibilité s'arrête.



Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud hébergeant l'interface active. De même, le basculement n'est pas déclenché par les services du Grid Manager ou du Tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes ne subissent que peu d'impact et puissent compter sur des comportements de nouvelle tentative normaux pour continuer à fonctionner.

Lorsque la panne est résolue et qu'une interface de priorité supérieure redevient disponible, les adresses VIP sont automatiquement déplacées vers l'interface de priorité la plus élevée disponible.

Comment les groupes HA de StorageGRID assurent une haute disponibilité

Vous pouvez utiliser des groupes à haute disponibilité (HA) pour fournir des connexions hautement disponibles à StorageGRID pour les données d'objets et pour une utilisation administrative.

- Un groupe HA peut fournir des connexions administratives hautement disponibles au Grid Manager ou au Tenant Manager.
- Un groupe HA peut fournir des connexions de données à haute disponibilité pour les clients S3.
- Un groupe HA ne contenant qu'une seule interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe HA ne peut garantir une haute disponibilité que si tous les nœuds qui le composent fournissent les mêmes services. Lorsque vous créez un groupe HA, ajoutez des interfaces provenant des types de nœuds qui fournissent les services dont vous avez besoin.

- **Nœuds d'administration** : Incluez le service Load Balancer et activez l'accès au Grid Manager ou au Tenant Manager.
- **Nœuds de passerelle** : Incluent le service Load Balancer.

Objectif du groupe HA	Ajoutez les nœuds de ce type au groupe HA
Accès à Grid Manager	• Nœud d'administration principal (Primary) • Nœuds d'administration non principaux Remarque : Le nœud d'administration principal doit être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Objectif du groupe HA	Ajoutez les nœuds de ce type au groupe HA
Accès uniquement à Tenant Manager	• Nœuds d'administration principaux ou non principaux
Accès client S3—Service Load Balancer	• Nœuds d'administration • Nœuds de passerelle
Accès client S3 pour "S3 Select"	• Appareils de services • Nœuds logiciels basés sur VMware Remarque : Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais ne sont pas requis.

Limitations liées à l'utilisation des groupes HA avec Grid Manager ou Tenant Manager

Si un service Grid Manager ou Tenant Manager tombe en panne, le basculement du groupe HA n'est pas déclenché.

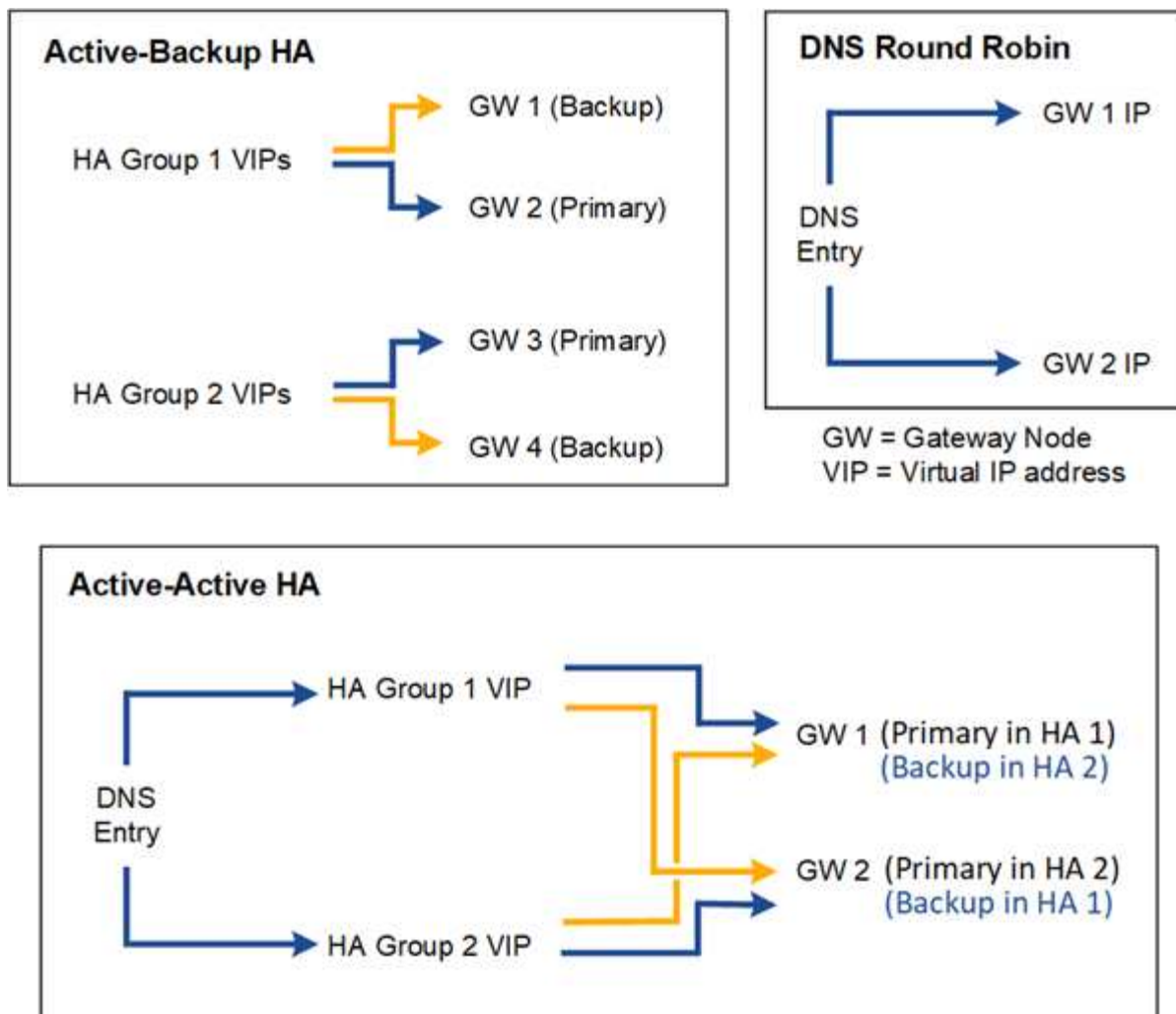
Si vous êtes connecté à Grid Manager ou à Tenant Manager lors d'un basculement, vous êtes déconnecté et devez vous reconnecter pour reprendre votre tâche.

Certaines opérations de maintenance sont impossibles lorsque le nœud d'administration principal est indisponible. En cas de basculement, vous pouvez utiliser le Grid Manager pour surveiller votre système StorageGRID.

Options de configuration pour les groupes à haute disponibilité StorageGRID

Les schémas suivants présentent des exemples de différentes façons dont vous pouvez configurer des groupes à haute disponibilité (HA). Chaque option comporte des avantages et des inconvénients.

Sur les schémas, le bleu indique l'interface principale du groupe HA et le jaune indique l'interface de secours du groupe HA.



Le tableau récapitule les avantages de chaque configuration HA présentée dans le schéma.

Configuration	Avantages	Inconvénients
HA actif-sauvegarde	- Géré par StorageGRID sans aucune dépendance externe. - Basculement rapide.	Dans un groupe HA, un seul nœud est actif. Au moins un nœud par groupe HA est inactif.
DNS Round Robin	- Augmentation du débit global. - Aucun hôte inactif.	- Basculement lent, pouvant dépendre du comportement du client. - Nécessite une configuration matérielle en dehors de StorageGRID. - Nécessite une vérification de l'état.
HA actif-actif	- Le trafic est réparti sur plusieurs groupes HA. - Débit agrégé élevé qui évolue avec le nombre de groupes HA. - Basculement rapide.	- Plus complexe à configurer. - Nécessite une configuration matérielle en dehors de StorageGRID. - Nécessite une vérification de l'état.

Configurez des groupes de haute disponibilité dans StorageGRID

Vous pouvez configurer des groupes à haute disponibilité (HA) pour fournir un accès hautement disponible aux services sur les nœuds d'administration ou les nœuds de passerelle.



Un système StorageGRID peut comporter un maximum de 255 groupes HA.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe HA, vous avez créé l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#).
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud dans un groupe HA, vous avez créé l'interface :
 - **Linux (avant l'installation du nœud)** : ["Créer des fichiers de configuration de nœud"](#)
 - **Linux (après installation du nœud)** : ["Ajouter des interfaces de tronc ou d'accès à un nœud"](#)
 - **VMware (après l'installation du nœud)** : ["Ajouter des interfaces de tronc ou d'accès à un nœud"](#)



« Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité \(IMT\) NetApp"](#).

Créer un groupe à haute disponibilité

Lorsque vous créez un groupe à haute disponibilité, vous sélectionnez une ou plusieurs interfaces et les organisez par ordre de priorité. Ensuite, vous attribuez une ou plusieurs adresses VIP au groupe.

Pour être incluse dans un groupe HA, une interface doit être dédiée à un nœud Gateway ou à un nœud Admin. Un groupe HA ne peut utiliser qu'une seule interface pour un nœud donné ; cependant, d'autres interfaces du même nœud peuvent être utilisées dans d'autres groupes HA.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Create**.

Saisissez les détails du groupe HA

Étapes

1. Donnez un nom unique au groupe HA.
2. Vous pouvez éventuellement saisir une description pour le groupe HA.
3. Sélectionnez **Continue**.

Ajouter des interfaces au groupe HA

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.



Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

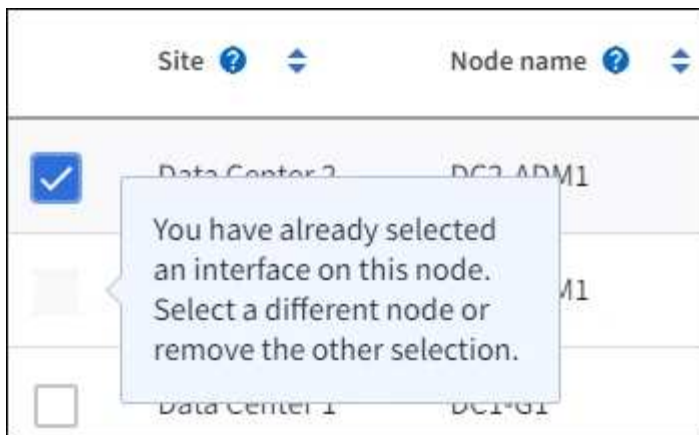
0 interfaces selected



Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse dans le tableau.

Recommandations pour la sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une seule interface pour un nœud.
- Si le groupe HA est destiné à la protection HA des services du nœud d'administration, qui incluent le Grid Manager et le Tenant Manager, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si le groupe HA est destiné à la protection HA du trafic client S3, sélectionnez des interfaces sur les nœuds Admin, les nœuds Gateway ou les deux.
- Si vous sélectionnez des interfaces sur différents types de nœuds, une note d'information s'affiche. Il vous est rappelé qu'en cas de basculement, les services fournis par le nœud précédemment actif pourraient ne pas être disponibles sur le nœud nouvellement actif. Par exemple, un nœud Gateway de secours ne peut pas assurer la protection HA des services du nœud Admin. De même, un nœud Admin de secours ne peut pas effectuer toutes les procédures de maintenance que le nœud Admin principal peut fournir.
- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L'infobulle 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 **Continue**.

Déterminez l'ordre de priorité

Si le groupe HA comprend plusieurs interfaces, vous pouvez déterminer quelle est l'interface principale et quelles sont les interfaces de secours (basculement). Si l'interface principale tombe en panne, les adresses VIP sont transférées vers l'interface prioritaire la plus élevée disponible. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface prioritaire suivante disponible, et ainsi de suite.

Étapes

1. Faites glisser les lignes de la colonne **Ordre de priorité** pour déterminer l'interface principale et les interfaces de secours.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node



Si le groupe HA donne accès au Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal comme interface principale. Certaines opérations de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

2. Sélectionnez **Continuer**.

Saisissez les adresses IP

Étapes

1. Dans le champ **Subnet CIDR**, spécifiez le sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32).

L'adresse réseau ne doit comporter aucun bit d'hôte activé. Par exemple, 192.16.0.0/22.



Si vous utilisez un préfixe 32 bits, l'adresse réseau VIP sert également d'adresse de passerelle et d'adresse VIP.

Enter details for the HA group

Subnet CIDR ⓘ

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ⓘ

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ⓘ

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. Si des clients administrateurs ou locataires S3 doivent accéder à ces adresses VIP depuis un sous-réseau différent, indiquez l'adresse IP de la passerelle. L'adresse de la passerelle doit se trouver dans le même sous-réseau VIP.

Les utilisateurs clients et administrateurs utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP et seront toutes actives simultanément sur l'interface active.

Vous devez fournir au moins une adresse IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer un groupe HA** et sélectionnez **Terminer**.

Le groupe HA est créé et vous pouvez désormais utiliser les adresses IP virtuelles configurées.

Prochaines étapes

Si vous utilisez ce groupe HA pour l'équilibrage de charge, créez un point de terminaison d'équilibrage de charge afin de déterminer le port et le protocole réseau et d'y associer les certificats requis. Voir "[Configurer les points de terminaison de l'équilibreur de charge](#)".

Modifier un groupe à haute disponibilité

Vous pouvez modifier un groupe à haute disponibilité (HA) pour changer son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous pourriez avoir besoin de modifier un groupe HA si vous souhaitez supprimer le nœud associé à une interface sélectionnée lors d'une procédure de mise hors service de site ou de nœud.

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.

La page des groupes de haute disponibilité affiche tous les groupes HA existants.

2. Cochez la case correspondant au groupe HA que vous souhaitez modifier.
3. Procédez comme suit, 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. Mettez à jour les adresses IP virtuelles du groupe HA.
 - b. Sélectionnez **Enregistrer**.
 - c. Sélectionnez **Terminer**.
5. Si vous avez sélectionné **Modifier le groupe HA** :
 - a. Vous pouvez éventuellement mettre à jour le nom ou la description du groupe.
 - b. Vous pouvez, si vous le souhaitez, sélectionner ou désélectionner les cases à cocher pour ajouter ou supprimer des interfaces.



Si le groupe HA donne accès au Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal comme interface principale. Certaines procédures de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

- c. Vous pouvez également faire glisser les lignes pour modifier l'ordre de priorité de l'interface principale et de toute interface de secours pour ce groupe HA.
- d. Vous pouvez éventuellement mettre à jour les adresses IP virtuelles.
- e. Sélectionnez **Enregistrer** puis sélectionnez **Terminer**.

Supprimer un groupe à haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes à haute disponibilité (HA) à la fois.



Vous ne pouvez pas supprimer un groupe HA s'il est lié à un point de terminaison d'équilibreur de charge. Pour supprimer un groupe HA, vous devez le retirer de tous les points de terminaison d'équilibreur de charge qui l'utilisent.

Pour éviter toute interruption de service, mettez à jour les applications clientes S3 concernées avant de supprimer un groupe HA. Mettez à jour chaque client pour qu'il se connecte à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe HA ou l'adresse IP qui a été configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Consultez la colonne **Points de terminaison de l'équilibreur de charge** pour chaque groupe HA que vous souhaitez supprimer. Si des points de terminaison de l'équilibreur de charge sont répertoriés :
 - a. Accédez à **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Cochez la case correspondant au point de terminaison.
 - c. Sélectionnez **Actions > Modifier le mode de liaison du point de terminaison**.
 - d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
 - e. Sélectionnez **Save changes**.
3. Si aucun point de terminaison d'équilibrage de charge n'est répertorié, cochez la case pour chaque groupe HA que vous souhaitez supprimer.
4. Sélectionnez **Actions > Supprimer le groupe HA**.
5. Vérifiez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

Tous les groupes HA que vous avez sélectionnés sont supprimés. Une bannière verte de succès apparaît sur la page Groupes de haute disponibilité.

Gérer l'équilibrage de charge

Découvrez l'équilibrage de charge StorageGRID

Vous pouvez utiliser l'équilibrage de charge pour gérer les charges de travail d'ingestion et de récupération des clients S3.

Qu'est-ce que l'équilibrage de charge ?

Lorsqu'une application cliente enregistre ou récupère des données depuis un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service d'équilibrage de charge StorageGRID est installé sur tous les nœuds d'administration et tous les nœuds de passerelle et assure l'équilibrage de charge de couche 7. Il effectue la terminaison TLS (Transport Layer Security) des requêtes client, les inspecte et établit de nouvelles connexions sécurisées avec les nœuds de stockage.

Le service d'équilibrage de charge de chaque nœud fonctionne indépendamment lors de la répartition du trafic client vers les nœuds de stockage. Grâce à un processus de pondération, le service d'équilibrage de charge achemine davantage de requêtes vers les nœuds de stockage disposant d'une plus grande disponibilité de processeur.



Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de charge recommandé, vous pouvez également intégrer un équilibreur de charge tiers. Pour plus d'informations, contactez votre représentant de compte NetApp ou consultez ["Utilisez des équilibreurs de charge tiers avec StorageGRID"](#).

De combien de nœuds d'équilibrage de charge avez-vous besoin ?

En bonne pratique, chaque site de votre système StorageGRID devrait comporter au moins deux nœuds avec le service d'équilibrage de charge. Par exemple, un site peut inclure deux nœuds de passerelle ou à la fois un nœud d'administration et un nœud de passerelle. Assurez-vous de disposer d'une infrastructure réseau, matérielle ou de virtualisation adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services, des nœuds bare metal ou des nœuds basés sur des machines virtuelles (VM).

Qu'est-ce qu'un point de terminaison d'équilibrage de charge ?

Un point de terminaison d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) que les requêtes entrantes et sortantes des applications clientes utiliseront pour accéder aux nœuds qui contiennent le service Load Balancer. Ce point de terminaison définit également le type de client (S3), le mode de liaison et, éventuellement, une liste de locataires autorisés ou bloqués.

Pour créer un point de terminaison d'équilibrage de charge, utilisez Grid Manager ou terminez la configuration S3 et les assistants FabricPool :

- ["Configurer les points de terminaison de l'équilibreur de charge"](#)
- ["Utilisez l'assistant de configuration S3"](#)
- ["Utilisez l'assistant de configuration FabricPool"](#)

Considérations relatives à la mise en cache de l'équilibreur de charge

La mise en cache améliore considérablement les performances lorsqu'une charge de travail traite un sous-ensemble de données et accède plusieurs fois aux objets. De plus, la mise en cache permet un accès distant au stockage d'objets sans déploiement complet de la grille. La mise en cache de l'équilibreur de charge est disponible uniquement pour les Gateway Nodes.

Lors de la création des points de terminaison de l'équilibreur de charge :

- N'activez la mise en cache que pour les charges de travail pouvant être mises en cache. Les charges de travail accédant plus fréquemment aux données non mises en cache qu'aux données mises en cache auront des performances inférieures à celles qui n'auraient pas été prises en charge par le cache. Dans certains cas, les charges de travail avec des taux élevés de réécriture et d'éviction peuvent également dépasser l'endurance d'écriture garantie du disque.
- Envisagez d'ajouter des points de terminaison ou des nœuds supplémentaires pour la mise en cache des charges de travail individuelles qui sont de bons candidats pour la mise en cache.
- Utilisez des points de terminaison distincts pour les charges de travail pouvant être mises en cache et celles qui ne le peuvent pas. Cette séparation garantit que les mécanismes de mise en cache sont appliqués correctement et n'interfèrent pas avec le traitement des données non mises en cache.
- Évaluez la pertinence d'une charge de travail pouvant être mise en cache en la dirigeant vers le point de terminaison compatible avec la mise en cache. Surveillez et vérifiez le taux d'accès au cache afin de déterminer si la charge de travail est adaptée à la mise en cache. Cette évaluation contribue à optimiser les performances et à garantir une utilisation efficace des ressources du cache.
- ["Examiner les journaux d'audit"](#) pour déterminer si une charge de travail existante serait un bon candidat

pour la mise en cache. Pour une période donnée, déterminez quel pourcentage des requêtes GET concerne des objets uniques. Pour être adaptée à la mise en cache, cette valeur doit être inférieure à 50 %.

Exemples de charges de travail qui pourraient être de bons candidats pour la mise en cache

- lacs de données
- Calcul haute performance (HPC)
- Entraînement IA/ML
- Réseaux de distribution de contenu (CDN)
- gestion des ressources média
- Production vidéo



- Plusieurs versions d'un même objet peuvent être mises en cache.
- Les opérations de lecture de plage sont prises en charge.

Exemples de charges de travail qui ne sont pas de bons candidats pour la mise en cache

- FabricPool
- Applications de sauvegarde
- hiérarchisation du stockage



Si un contenu quelconque à servir par le cache nécessite un chiffrement au repos, "[activer le chiffrement du nœud ou du disque](#)" sur le nœud de cache.

Types d'objets et de requêtes qui ne seront pas mis en cache

- Le `response-content-encoding` paramètre de requête
- Le `partNumber` paramètre de requête
- En-têtes conditionnels
 - `If-Match`
 - `If-Modified-Since`
 - `If-None-Match`
 - `If-Unmodified-Since`
- Les requêtes qui ont été chiffrées au repos avec l'un des éléments suivants :
 - SSE (chiffrement côté serveur avec des clés gérées par StorageGRID)
 - SSE-C (chiffrement côté serveur avec clés fournies par le client)
 - Chiffrement des objets stockés

Toute requête qui n'est pas mise en cache est transmise à un LDR en amont comme si le cache n'était pas activé.

Informations connexes

- "[Dépannez la mise en cache de l'équilibreur de charge](#)"

- Pour plus d'informations sur la mise en cache de l'équilibreur de charge, contactez le support technique.

Considérations relatives au port

Le port d'un point de terminaison d'équilibrage de charge est par défaut 10433 pour le premier point de terminaison que vous créez, mais vous pouvez spécifier n'importe quel port externe inutilisé entre 1 et 65535. Si vous utilisez le port 80 ou 443, le point de terminaison utilisera le service Load Balancer uniquement sur les Gateway Nodes. Ces ports sont réservés sur les Admin Nodes. Si vous utilisez le même port pour plus d'un point de terminaison, vous devez spécifier un mode de liaison différent pour chaque point de terminaison.

Les ports utilisés par d'autres services de grid ne sont pas autorisés. Voir ["Ports internes de StorageGRID"](#).

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le chiffrement Transport Layer Security (TLS). La connexion à StorageGRID sans chiffrement TLS est possible, mais déconseillée, notamment en environnement de production. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID, vous devez choisir **HTTPS**.

Considérations relatives aux certificats des points de terminaison de l'équilibreur de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le point de terminaison de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Vous pouvez utiliser l'une de ces trois options lors de la création du point de terminaison de l'équilibreur de charge :

- **Téléchargez un certificat signé (recommandé).** Ce certificat peut être signé par une autorité de certification (CA) publique ou privée. Utiliser un certificat de serveur CA public pour sécuriser la connexion est la bonne pratique. Contrairement aux certificats générés, les certificats signés par une CA peuvent être renouvelés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

Vous devez obtenir les fichiers suivants avant de créer le point de terminaison de l'équilibreur de charge :

- Le fichier de certificat serveur personnalisé.
- Le fichier de clé privée du certificat serveur personnalisé.
- En option, un ensemble de certificats CA provenant de chaque autorité de certification émettrice intermédiaire.
- **Générez un certificat auto-signé.**
- **Utilisez le certificat S3 global StorageGRID.** Vous devez importer ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le point de terminaison de l'équilibreur de charge. Voir ["Configurer les certificats de l'API S3"](#).

De quelles valeurs avez-vous besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications clientes S3 utiliseront pour accéder au point de terminaison.

L'entrée **Subject DN** (Nom distinctif) du certificat doit inclure le nom de domaine complet que l'application cliente utilisera pour StorageGRID. Par exemple :

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```


Conformément aux exigences, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et les nœuds de passerelle exécutant le service Load Balancer. Par exemple, *.storagegrid.example.com utilise le caractère générique * pour représenter adm1.storagegrid.example.com et gn1.storagegrid.example.com.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, le certificat doit également inclure une entrée **Nom alternatif** pour chaque "nom de domaine du terminal S3" que vous avez configuré, y compris tout nom générique. Par exemple :

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Si vous utilisez des caractères génériques pour les noms de domaine, consultez la ["Recommandations pour le renforcement de la sécurité des certificats de serveur"](#).

Vous devez également définir une entrée DNS pour chaque nom figurant dans le certificat de sécurité.

Comment gérer les certificats qui expirent ?



Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application risque de perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration de certificat, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que les alertes **Expiration of load balancer endpoint certificate** et **Expiration of global server certificate for S3 API**.
- Veillez à toujours synchroniser les versions du certificat de StorageGRID et de l'application S3. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez également remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utilisez un certificat signé par une autorité de certification (CA) publique. Si vous utilisez un certificat signé par une CA, vous pouvez remplacer les certificats arrivant bientôt à expiration sans interruption de service.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement à la fois dans StorageGRID et dans l'application S3 avant l'expiration du certificat existant.

Considérations relatives au mode de liaison

Le mode de liaison permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un point de terminaison d'équilibreur de charge. Si un point de terminaison utilise un mode de liaison, les applications clientes ne peuvent accéder au point de terminaison que si elles utilisent une adresse IP autorisée ou son domaine complet (FQDN) correspondant. Les applications clientes utilisant toute autre adresse IP ou tout autre FQDN ne peuvent pas accéder au point de terminaison.

Vous pouvez spécifier l'un des modes de liaison suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au point de terminaison via l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un domaine complet (FQDN) correspondant. Utilisez ce paramètre sauf si vous devez restreindre l'accessibilité d'un point de terminaison.

- **Adresses IP virtuelles des groupes HA.** Les applications clientes doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe HA.
- **Interfaces de nœud.** Les clients doivent utiliser les adresses IP (ou les domaines complets correspondants) des interfaces de nœud sélectionnées.
- **Type de nœud.** En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud de passerelle.

Considérations relatives à l'accès des locataires

Le contrôle d'accès des locataires est une fonctionnalité de sécurité optionnelle qui vous permet de contrôler quels comptes locataires StorageGRID peuvent utiliser un point de terminaison d'équilibrage de charge pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un point de terminaison (par défaut), ou spécifier une liste de locataires autorisés ou bloqués pour chaque point de terminaison.

Vous pouvez utiliser cette fonctionnalité pour offrir une meilleure isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonctionnalité pour garantir que les documents ultra-confidentiels ou hautement classifiés appartenant à un locataire restent totalement inaccessibles aux autres locataires.



Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la requête du client ; si aucune clé d'accès n'est fournie dans le cadre de la requête (comme dans le cas d'accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès locataire

Pour comprendre le fonctionnement de cette fonction de sécurité, considérez l'exemple suivant :

1. Vous avez créé deux points de terminaison d'équilibrage de charge, comme suit :
 - Point de terminaison **public** : utilise le port 10443 et permet l'accès à tous les tenants.
 - Point d'accès **Top secret** : utilise le port 10444 et autorise l'accès uniquement au locataire **Top secret**. Tous les autres locataires sont bloqués de l'accès à ce point d'accès.
2. Le `top-secret.pdf` se trouve dans un compartiment appartenant au locataire **Top secret**.

Pour accéder à `top-secret.pdf`, un utilisateur du locataire **Top secret** peut envoyer une requête GET à `https://w.x.y.z:10444/top-secret.pdf`. Ce locataire étant autorisé à utiliser le point de terminaison 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire envoie la même requête à la même URL, il reçoit immédiatement un message Accès refusé. L'accès est refusé même si les identifiants et la signature sont valides.

disponibilité du processeur

Le service d'équilibrage de charge sur chaque nœud d'administration et de passerelle fonctionne indépendamment lors de l'acheminement du trafic S3 vers les nœuds de stockage. Grâce à un processus de pondération, le service d'équilibrage de charge dirige davantage de requêtes vers les nœuds de stockage disposant d'une plus grande disponibilité CPU. Les informations sur la charge CPU des nœuds sont mises à jour toutes les quelques minutes, mais la pondération peut être actualisée plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids minimale, même si un nœud signale 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 de Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge StorageGRID

Les points de terminaison de l'équilibreur de charge déterminent les ports et les protocoles réseau que les clients S3 peuvent utiliser pour se connecter à l'équilibreur de charge StorageGRID sur les nœuds Gateway et Admin. Vous pouvez également utiliser ces points de terminaison pour accéder au Grid Manager, au Tenant Manager ou aux deux.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Vous avez examiné le ["considérations relatives à l'équilibrage de charge"](#).
- Si vous avez précédemment remappé un port que vous prévoyez d'utiliser pour le point de terminaison de l'équilibreur de charge, vous avez ["suppression du remappage de port"](#).
- Vous avez créé les groupes de haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HA sont recommandés, mais non obligatoires. Voir ["Gérer les groupes à haute disponibilité"](#).
- Si le point de terminaison de l'équilibreur de charge sera utilisé par ["Locataires S3 pour S3 Select"](#), il ne doit pas utiliser les adresses IP ni les FQDN de nœuds bare-metal. Seuls les appliances de services et les nœuds logiciels basés sur VMware sont autorisés pour les points de terminaison de l'équilibreur de charge utilisés pour S3 Select.
- Vous avez configuré les interfaces VLAN que vous prévoyez d'utiliser. Voir ["Configurer les interfaces VLAN"](#).
- Si vous créez un point de terminaison HTTPS (recommandé), vous disposez des informations pour le certificat du serveur.



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

- Pour télécharger un certificat, vous avez besoin du certificat serveur, de la clé privée du certificat et, éventuellement, d'un bundle d'autorité de certification (CA bundle).
- Pour générer un certificat, vous avez besoin de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au point de terminaison. Vous devez également connaître le sujet (Distinguished Name).
- Si vous souhaitez utiliser le certificat de l'API StorageGRID S3 (qui peut également être utilisé pour les connexions directes aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir ["Configurer les certificats de l'API S3"](#).

Créer un point de terminaison d'équilibrage de charge

Chaque point de terminaison d'équilibrage de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les points de terminaison d'équilibrage de charge de l'interface de gestion spécifient un port, un type d'interface et un réseau Client Network non approuvé.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
2. Pour créer un point de terminaison pour un client S3, sélectionnez l'onglet **S3 client**.
3. Pour créer un point de terminaison permettant d'accéder au Grid Manager, au Tenant Manager ou aux deux, sélectionnez l'onglet **Management interface**.
4. Sélectionnez **Create**.

Saisissez les détails du point de terminaison

Étapes

1. Sélectionnez les instructions appropriées pour saisir les détails du type de point de terminaison que vous souhaitez créer.

Client S3

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé compris entre 1 et 65535. Si vous saisissez 80 ou 8443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, sauf si vous avez libéré le port 8443. Vous pouvez alors utiliser le port 8443 comme point de terminaison S3, et le port sera configuré à la fois sur les nœuds de passerelle et d'administration.
Type de client	Doit être S3 .
Protocole réseau	Le protocole réseau que les clients utiliseront lorsqu'ils se connecteront à ce point de terminaison. • Sélectionnez HTTPS pour une communication sécurisée et chiffrée TLS (recommandé). Vous devez associer un certificat de sécurité avant de pouvoir enregistrer le point de terminaison. • Sélectionnez HTTP pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille hors production.
Activer la mise en cache	Activer ou désactiver "mise en cache sur les nœuds de passerelle" pour ce point de terminaison d'équilibrage de charge. En cas de problème de mise en cache, veuillez vous référer à "Dépannez la mise en cache de l'équilibreur de charge".

Interface de gestion

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.

Champ	Description
Port	Le port StorageGRID que vous souhaitez utiliser pour accéder au Grid Manager, au Tenant Manager ou aux deux. • Gestionnaire de grille : 8443 • Gestionnaire de locataires : 9443 • Gestionnaire de grille et gestionnaire de locataires : 443 Remarque : Vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio pour l'interface StorageGRID à laquelle vous accéderez à l'aide de ce point de terminaison.
Réseau de clients non fiables	Sélectionnez Oui si ce point de terminaison doit être accessible aux réseaux clients non approuvés. Sinon, sélectionnez Non. Lorsque vous sélectionnez Oui, le port est ouvert sur tous les réseaux clients non approuvés. Remarque : Vous ne pouvez configurer un port pour qu'il soit ouvert ou fermé aux réseaux clients non approuvés que lors de la création du point de terminaison de l'équilibreur de charge.

1. Sélectionnez **Continue**.

Sélectionnez un mode de liaison

Étapes

1. Sélectionnez un mode de liaison pour le point de terminaison afin de contrôler la manière dont le point de terminaison est accessible en utilisant n'importe quelle adresse IP ou en utilisant des adresses IP et des interfaces réseau spécifiques.

Certains modes de liaison sont disponibles pour les points de terminaison clients ou les points de terminaison d'interface de gestion. Tous les modes pour les deux types de points de terminaison sont répertoriés ici.

Mode	Description
Global (par défaut pour les points de terminaison clients)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global sauf si vous devez restreindre l'accessibilité de ce point de terminaison.

Mode	Description
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud (points de terminaison clients uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.
Tous les nœuds d'administration (par défaut pour les points de terminaison de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration pour accéder à ce point de terminaison.

Si plusieurs points de terminaison utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel point de terminaison utiliser : **Virtual IPs of HA groups** > **Interfaces de nœud** > **Type de nœud** > **Global**.

Si vous créez des points de terminaison d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **Virtual IPs of HA groups**, sélectionnez un ou plusieurs groupes HA.

Si vous créez des points de terminaison d'interface de gestion, sélectionnez les VIP associés uniquement aux Admin Nodes.

3. Si vous avez sélectionné **Interfaces de nœud**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce point de terminaison.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit Admin Nodes, qui comprend à la fois le primary Admin Node et tous les non-primary Admin Nodes, soit Gateway Nodes.

Contrôler l'accès des locataires



Un point de terminaison d'interface de gestion ne peut contrôler l'accès des locataires que lorsque le point de terminaison possède le [type d'interface de Tenant Manager](#).

Étapes

1. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de comptes locataires. Après avoir ajouté des comptes locataires, vous pouvez modifier le point de terminaison de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

- Si vous créez un point de terminaison **HTTP**, vous n'avez pas besoin d'associer un certificat. Sélectionnez **Créer** pour ajouter le nouveau point de terminaison d'équilibrage de charge. Ensuite, accédez à [Après avoir terminé](#). Sinon, sélectionnez **Continuer** pour associer le certificat.

Joindre le certificat

Étapes

- Si vous créez un point de terminaison **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au point de terminaison.

Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur le nœud d'administration ou les nœuds de passerelle.

- **Téléverser un certificat.** Sélectionnez cette option si vous avez des certificats personnalisés à téléverser.
- **Générer un certificat.** Sélectionnez cette option si vous disposez des informations nécessaires pour générer un certificat personnalisé.
- **Utiliser le certificat StorageGRID S3.** Sélectionnez cette option si vous souhaitez utiliser le certificat global de l'API S3, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 par défaut, qui est signé par l'AC du grid, par un certificat personnalisé signé par une autorité de certification externe. Voir "[Configurer les certificats de l'API S3](#)".

- **Utiliser le certificat d'interface de gestion.** Sélectionnez cette option si vous souhaitez utiliser le certificat d'interface de gestion global, qui peut également être utilisé pour les connexions directes aux nœuds d'administration.
- Si vous n'utilisez pas le certificat S3 StorageGRID, téléchargez-le ou générez-le.

Télécharger le certificat

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé au format PEM.
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (.key).



Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **CA bundle** : Fichier optionnel unique contenant les certificats de chaque autorité de certification (CA) intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA encodés en 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 importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans son propre onglet.

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

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Créer**. + Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le point de terminaison.

Générer un certificat

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.

Champ	Description
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. Remarque : Laissez cette case cochée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

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 son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Create**.

Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce point de terminaison.

Après avoir terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que celui-ci inclut un enregistrement permettant d'associer le nom de domaine complet (FQDN) de StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

L'adresse IP que vous saisissez dans l'enregistrement DNS dépend du fait que vous utilisiez ou non un groupe HA de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe HA, les clients se connecteront aux adresses IP virtuelles de ce groupe HA.
- Si vous n'utilisez pas de groupe HA, les clients se connecteront au service d'équilibrage de charge StorageGRID en utilisant l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point de terminaison requis, y compris les noms génériques.

2. Fournissez aux clients S3 les informations nécessaires pour se connecter au point de terminaison :

- Numéro de port
- nom de domaine complet ou adresse IP
- Tous les détails de certificat requis

Afficher et modifier les points de terminaison de l'équilibreur de charge

Vous pouvez consulter les détails des points de terminaison d'équilibrage de charge existants, y compris les métadonnées du certificat d'un point de terminaison sécurisé. Vous pouvez modifier certains paramètres d'un point de terminaison.

- Pour consulter les informations de base de tous les points de terminaison de l'équilibreur de charge, consultez les tableaux de la page Points de terminaison de l'équilibreur de charge.
- Pour afficher tous les détails d'un point de terminaison spécifique, y compris les métadonnées du certificat, sélectionnez le nom du point de terminaison dans le tableau. Les informations affichées varient selon le type de point de terminaison et la façon dont il est configuré.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

[Remove](#)

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

[Edit binding mode](#)

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Pour modifier un point de terminaison, utilisez le menu **Actions** sur la page des points de terminaison de l'équilibreur de charge.



Si vous perdez l'accès à Grid Manager lors de la modification du port d'un point de terminaison d'interface de gestion, mettez à jour l'URL et le port pour rétablir l'accès.



Après avoir modifié un point de terminaison, vous devrez peut-être attendre jusqu'à 15 minutes pour que vos modifications soient appliquées à tous les nœuds.

Tâche	Menu Actions	Page de détails
Modifier le nom du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le nom du point de terminaison. c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez Enregistrer.
Modifier le port du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le port du point de terminaison. c. Veuillez saisir un numéro de port valide. d. Sélectionnez Enregistrer.	<i>n/a</i>
Modifier le mode de liaison du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le mode de liaison du point de terminaison. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez Save changes.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez Modifier le mode de liaison. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez Save changes.
Modifier le certificat du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le certificat du point de terminaison. c. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. d. Sélectionnez Save changes.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet Certificat. c. Sélectionnez Modifier le certificat. d. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. e. Sélectionnez Save changes.

Tâche	Menu Actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier l'accès du locataire . c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. d. Sélectionnez Save changes .	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet Accès locataire . c. Sélectionnez Modifier l'accès du locataire . d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. e. Sélectionnez Save changes .

Supprimez les points de terminaison de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs points de terminaison à l'aide du menu **Actions**, ou vous pouvez supprimer un seul point de terminaison à partir de la page de détails.



Pour éviter toute interruption de service client, mettez à jour les applications clientes S3 concernées avant de supprimer un point de terminaison d'équilibreur de charge. Mettez à jour chaque client pour qu'il se connecte à l'aide d'un port attribué à un autre point de terminaison d'équilibreur de charge. Veillez également à mettre à jour les informations de certificat requises.



Si vous perdez l'accès à Grid Manager lors de la suppression d'un point de terminaison d'interface de gestion, mettez à jour l'URL.

- Pour supprimer un ou plusieurs points de terminaison :
 - Sur la page de l'équilibreur de charge, cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.
 - Sélectionnez **Actions > Supprimer**.
 - Sélectionnez **OK**.
- Pour supprimer un point de terminaison de la page de détails :
 - Sur la page de l'équilibreur de charge, sélectionnez le nom du point de terminaison.
 - Sélectionnez **Supprimer** sur la page de détails.
 - Sélectionnez **OK**.

Configurez les noms de domaine des points de terminaison S3 dans StorageGRID

Pour prendre en charge les requêtes de type hébergement virtuel S3, vous devez utiliser le Grid Manager pour configurer la liste des noms de domaine des points de terminaison S3 auxquels les clients S3 se connectent.



L'utilisation d'une adresse IP comme nom de domaine d'endpoint n'est pas prise en charge. Les prochaines versions empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez confirmé qu'aucune mise à niveau de la grille n'est en cours.



Ne modifiez pas la configuration du nom de domaine pendant une mise à niveau du grid.

À propos de cette tâche

Pour permettre aux clients d'utiliser les noms de domaine des points de terminaison S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez Grid Manager pour ajouter les noms de domaine des points de terminaison S3 au système StorageGRID.
- Assurez-vous que le ["certificat que le client utilise pour les connexions HTTPS à StorageGRID"](#) est signé pour tous les noms de domaine requis par le client.

Par exemple, si le point de terminaison est `s3.company.com`, vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` point de terminaison et le nom alternatif de sujet générique (SAN) du point de terminaison : `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et assurez-vous que ces enregistrements référencent tous les noms de domaine de point de terminaison S3 requis, y compris tout nom générique (wildcard).



Les clients peuvent se connecter à StorageGRID via l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou via l'adresse IP virtuelle d'un groupe à haute disponibilité. Vous devez comprendre comment les applications clientes se connectent à la grille afin d'inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) à la grille peuvent utiliser l'un ou l'autre de ces certificats :

- Les clients qui se connectent à un point de terminaison d'équilibreur de charge peuvent utiliser un certificat personnalisé pour ce point de terminaison. Chaque point de terminaison d'équilibreur de charge peut être configuré pour reconnaître différents noms de domaine de point de terminaison S3.
- Les clients qui se connectent à un point de terminaison d'équilibreur de charge ou directement à un nœud de stockage peuvent personnaliser le certificat d'API S3 global pour inclure tous les noms de domaine de point de terminaison S3 requis.



Si vous n'ajoutez pas de noms de domaine de point de terminaison S3 et que la liste est vide, la prise en charge des requêtes de type hébergement virtuel S3 est désactivée.

Ajouter un nom de domaine de point de terminaison S3

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine des endpoints S3**.
2. Saisissez le nom de domaine dans le champ **Nom de domaine 1**. Sélectionnez **Ajouter un autre nom de domaine** pour ajouter d'autres noms de domaine.

3. Sélectionnez **Enregistrer**.
4. Assurez-vous que les certificats serveur utilisés par les clients correspondent aux noms de domaine des points de terminaison S3 requis.
 - Si les clients se connectent à un point de terminaison d'équilibreur de charge qui utilise son propre certificat, "[mettre à jour le certificat associé au point de terminaison](#)".
 - Si les clients se connectent à un point de terminaison d'équilibreur de charge qui utilise le certificat d'API S3 global ou directement aux nœuds de stockage, "[mettre à jour le certificat global de l'API S3](#)".
5. Ajoutez les enregistrements DNS nécessaires pour garantir que les requêtes de nom de domaine des points de terminaison puissent être résolues.

Résultat

Désormais, lorsque les clients utilisent le point de terminaison `bucket.s3.company.com`, le serveur DNS résout le point de terminaison correct et le certificat authentifie le point de terminaison comme prévu.

Renommer un nom de domaine d'endpoint S3

Si vous modifiez un nom utilisé par les applications S3, les requêtes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine des endpoints S3**.
2. Sélectionnez le champ du nom de domaine que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimer un nom de domaine de point de terminaison S3

Si vous supprimez un nom utilisé par les applications S3, les requêtes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **Configuration > Réseau > Noms de domaine des endpoints S3**.
2. Sélectionnez l'icône de suppression  à côté du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations connexes

- "[Utilisez l'API REST S3](#)"
- "[Afficher les adresses IP](#)"
- "[Configurer les groupes à haute disponibilité](#)"

Adresses IP et ports pour les connexions client StorageGRID

Pour stocker ou récupérer des objets, les applications clientes S3 se connectent au service Load Balancer, qui est inclus sur tous les Admin Nodes et Gateway Nodes, ou au service Local Distribution Router (LDR), qui est inclus sur tous les Storage Nodes.

Les applications clientes peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud du réseau et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes de haute disponibilité

(HA) de nœuds d'équilibrage de charge afin de fournir des connexions hautement disponibles utilisant des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un domaine complet (FQDN, fully qualified domain name) plutôt que d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Ce tableau récapitule les différents modes de connexion des clients à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Si vous avez déjà créé des points de terminaison d'équilibrage de charge et des groupes de haute disponibilité (HA), consultez [Où trouver des adresses IP](#) pour localiser ces valeurs dans le Grid Manager.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HA	Équilibreur de charge	Adresse IP virtuelle d'un groupe HA	Port attribué au point de terminaison de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud passerelle	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP: 18084

Exemples d'URL

Pour connecter une application cliente au point de terminaison de l'équilibreur de charge d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

`https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.5 et que le numéro de port du point de terminaison de l'équilibreur de charge est 10443, une application peut utiliser l'URL suivante pour se connecter à StorageGRID :

`https://192.0.2.5:10443`

Où trouver des adresses IP

1. Connectez-vous au Gestionnaire de grille en utilisant un ["navigateur Web pris en charge"](#).
2. Pour trouver l'adresse IP d'un nœud de grille :
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.

- c. Sélectionnez l'onglet **Overview**.
- 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 correspondances d'interface.

Vous pouvez établir des connexions depuis des applications clientes vers n'importe laquelle des adresses IP de la liste :

- **eth0**: Réseau Grid
- **eth1**: Réseau d'administration (facultatif)
- **eth2**: Réseau client (facultatif)



Si vous consultez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe à haute disponibilité, l'adresse IP virtuelle du groupe HA est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe à haute disponibilité :
 - a. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
 - b. Dans le tableau, notez l'adresse IP virtuelle du groupe HA.
4. Pour trouver le numéro de port d'un point de terminaison d'équilibreur de charge :
 - a. Sélectionnez **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Notez le numéro de port du point de terminaison que vous souhaitez utiliser.



Si le numéro de port est 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et les nœuds d'administration.

- c. Sélectionnez le nom du point de terminaison dans le tableau.
- d. Vérifiez que le **type de client** (S3) correspond à l'application cliente qui utilisera le point de terminaison.

Gérer les réseaux et les connexions

Configurer les paramètres réseau de StorageGRID

Vous pouvez configurer différents paramètres réseau depuis le Grid Manager afin d'optimiser le fonctionnement de votre système StorageGRID.

Configurer les interfaces VLAN

Vous pouvez "[créer des interfaces de réseau local virtuel \(VLAN\)](#)" isoler et partitionner le trafic pour des raisons de sécurité, de flexibilité et de performance. Chaque interface VLAN est associée à une ou plusieurs interfaces parentes sur les Admin Nodes et les Gateway Nodes. Vous pouvez utiliser les interfaces VLAN dans les groupes HA et dans les points de terminaison d'équilibrage de charge pour séparer le trafic client ou d'administration par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser ["politiques de classification du trafic"](#) pour identifier et gérer différents types de trafic réseau, y compris le trafic lié à des compartiments spécifiques, des locataires, des sous-réseaux clients ou des points de terminaison d'équilibrage de charge. Ces politiques peuvent aider à limiter et à surveiller le trafic.

Directives pour les réseaux StorageGRID

Vous pouvez utiliser Grid Manager pour configurer et gérer les réseaux et les connexions StorageGRID.

Consultez ["Configurer les connexions client S3"](#) pour savoir comment connecter des clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud de grille, ce qui vous permet de configurer le réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, consultez ["Directives de mise en réseau"](#).

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour tout le trafic interne de StorageGRID. Il assure la connectivité entre tous les nœuds de la grille, sur l'ensemble des 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 aux protocoles clients. Le réseau d'administration est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir un accès aux applications clientes S3, afin que le réseau Grid puisse être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Lignes directrices

- Chaque nœud StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est affecté.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une seule passerelle par réseau et par nœud de grille est prise en charge, et elle doit se trouver sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe au niveau de la passerelle, si nécessaire.
- Sur chaque nœud, chaque réseau est associé à une interface réseau spécifique.

Réseau	Nom de l'interface
Grid	eth0

Réseau	Nom de l'interface
Administrateur (facultatif)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à un StorageGRID appliance, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, consultez les instructions d'installation de votre appliance.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, alors 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client ne devient opérationnel que lorsque le nœud de grille a rejoint la grille
- Le réseau d'administration peut être configuré lors du déploiement du nœud de la grille pour permettre l'accès à l'interface utilisateur d'installation avant que la grille ne soit entièrement installée.

Interfaces optionnelles

Vous pouvez éventuellement ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pourriez vouloir ajouter une interface trunk à un nœud Admin ou Gateway, afin de pouvoir utiliser ["Interfaces VLAN"](#) pour segmenter le trafic appartenant à différentes applications ou locataires. Ou, vous pourriez vouloir ajouter une interface d'accès à utiliser dans un ["groupe à haute disponibilité \(HA\)"](#).

Pour ajouter des interfaces trunk ou d'accès, consultez les informations suivantes :

- **VMware (après installation du nœud)** : ["VMware : Ajouter des interfaces trunk ou d'accès à un nœud"](#)
 - **Linux (avant l'installation du nœud)** : ["Créer des fichiers de configuration de nœud"](#)
 - **Linux (après installation du nœud)** : ["Ajouter des interfaces de tronc ou d'accès à un nœud"](#)



« Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité \(IMT\) NetApp"](#).

Afficher les adresses IP dans StorageGRID

Vous pouvez consulter l'adresse IP de chaque nœud de votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud via la ligne de commandes et effectuer diverses opérations de maintenance.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

Pour plus d'informations sur la modification des adresses IP, consultez ["Configurer les adresses IP"](#).

Étapes

1. Sélectionnez **Nodes** > **grid node** > **Overview**.
2. Sélectionnez **Afficher plus** à droite du titre IP Addresses.

Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  **Connected**

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ^	IP address ^
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ^	Severity ? ^	Time triggered ^	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configure the VLAN interfaces in StorageGRID

Créez des interfaces VLAN (réseau local virtuel) sur les nœuds d'administration et les nœuds passerelle, puis utilisez-les dans des groupes HA et des points de terminaison d'équilibrage de charge afin d'isoler et de partitionner le trafic pour la sécurité, la flexibilité et la performance. Les nœuds sélectionnés dans le groupe HA peuvent utiliser les interfaces VLAN pour partager jusqu'à 10 adresses IP virtuelles, de sorte que si un nœud tombe en panne, un autre nœud prend en charge le trafic à destination et en provenance des adresses IP virtuelles.

Considerations relatives aux interfaces VLAN

- Vous créez une interface VLAN en saisissant un ID de VLAN et en choisissant une interface parente sur un

ou plusieurs nœuds.

- Une interface parente doit être configurée comme interface trunk au niveau du commutateur.
- Une interface parente peut être le Grid Network (eth0), le Client Network (eth2) ou une interface trunk supplémentaire pour la VM ou l'hôte bare-metal (par exemple, ens256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parente pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface Grid Network et l'interface Client Network sur le même Gateway Node comme interface parente pour un même VLAN.
- Si l'interface VLAN est destinée au trafic du nœud d'administration, y compris le trafic lié au Grid Manager et au Tenant Manager, sélectionnez uniquement les interfaces des nœuds d'administration.
- Si l'interface VLAN est destinée au trafic client S3, sélectionnez les interfaces sur les nœuds d'administration ou les nœuds de passerelle.
- Si vous devez ajouter des interfaces de tronc, consultez les informations suivantes :
 - **VMware (après installation du nœud)** : ["VMware : Ajouter des interfaces trunk ou d'accès à un nœud"](#)
 - **Linux (avant l'installation du nœud)** : ["Créer des fichiers de configuration de nœud"](#)
 - **Linux (après installation du nœud)** : ["Ajouter des interfaces de tronc ou d'accès à un nœud"](#)



« Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité \(IMT\) NetApp"](#).

Créer une interface VLAN

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Une interface trunk a été configurée sur le réseau et connectée à la machine virtuelle ou au nœud Linux. Vous connaissez le nom de l'interface trunk.
- Vous connaissez l'identifiant du VLAN que vous configurez.

À propos de cette tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces trunk et un ou plusieurs VLAN afin de séparer le trafic client ou d'administration appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un identifiant numérique ou un tag. 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 permettant aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID du VLAN et sélectionnez les interfaces parentes (trunk) sur un ou plusieurs nœuds.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration > Réseau > Interfaces VLAN**.
2. Sélectionnez **Create**.

Saisissez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN sur votre réseau. Vous pouvez saisir 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 de VLAN 200 pour le trafic d'administration sur un site et le même ID pour le trafic client sur un autre site. Vous pouvez créer des interfaces VLAN distinctes avec des ensembles d'interfaces parentes différents 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.

2. Vous pouvez éventuellement saisir une brève description pour l'interface VLAN.
3. Sélectionnez **Continue**.

Choisissez les interfaces parentes

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et les nœuds passerelle à chaque site de votre grille. Les interfaces du réseau d'administration (eth1) ne peuvent pas être utilisées comme interfaces parentes et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parentes auxquelles associer ce VLAN.

Par exemple, vous pourriez vouloir attacher un VLAN à l'interface Client Network (eth2) pour un Gateway Node et un Admin Node.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

Search...

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

Previous

Continue

2. Sélectionnez **Continue**.

Confirmez les paramètres

Étapes

1. Vérifiez la configuration et apportez les modifications nécessaires.
 - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **Saisir les détails du VLAN** en haut de la page.
 - Si vous devez modifier une interface parente, sélectionnez **Choisir les interfaces parentes** en haut de la page ou sélectionnez **Précédent**.
 - Si vous devez supprimer une interface parente, sélectionnez l'icône de la corbeille .
2. Sélectionnez **Enregistrer**.
3. Attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse comme sélection sur la page des groupes de haute disponibilité et soit répertoriée dans le tableau **Interfaces réseau** pour le nœud (**Nœuds** > **parent interface node** > **Réseau**).

Modifier une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID VLAN ou la description.
- Ajouter ou supprimer des interfaces parentes.

Par exemple, vous pourriez vouloir supprimer une interface parente d'une interface VLAN si vous prévoyez de mettre hors service le nœud associé.

Remarque :

- Vous ne pouvez pas modifier l'ID d'un VLAN si l'interface VLAN est utilisée dans un groupe HA.
- Vous ne pouvez pas supprimer une interface parente si celle-ci est utilisée dans un groupe HA.

Par exemple, supposons que le VLAN 200 soit connecté aux interfaces parentes 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 parente inutilisée du nœud B, mais vous ne pouvez pas supprimer l'interface parente utilisée du nœud A.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN que vous souhaitez modifier. Ensuite, sélectionnez **Actions** > **Modifier**.
3. Vous pouvez éventuellement mettre à jour l'ID du VLAN ou la description. Ensuite, sélectionnez **Continuer**.

Vous ne pouvez pas mettre à jour un ID de VLAN si le VLAN est utilisé dans un groupe HA.

4. Vous pouvez cocher ou décocher les cases pour ajouter des interfaces parentes ou supprimer les interfaces inutilisées. Ensuite, sélectionnez **Continuer**.
5. Vérifiez la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprimer une interface VLAN

Vous pouvez supprimer une ou plusieurs interfaces VLAN.

Vous ne pouvez pas supprimer une interface VLAN si elle est actuellement utilisée dans un groupe HA. Vous devez retirer l'interface VLAN du groupe HA avant de pouvoir la supprimer.

Pour éviter toute interruption du trafic client, envisagez de faire l'une des actions suivantes :

- Ajoutez une nouvelle interface VLAN au groupe HA avant de supprimer cette interface VLAN.
- Créez un nouveau groupe HA qui n'utilise pas cette interface VLAN.
- Si l'interface VLAN que vous souhaitez supprimer est actuellement l'interface active, modifiez le groupe HA. Déplacez l'interface VLAN que vous souhaitez supprimer en bas de la liste de priorité. Attendez que la communication soit établie sur la nouvelle interface principale, puis supprimez l'ancienne interface du groupe HA. Enfin, supprimez l'interface VLAN sur ce nœud.

Étapes

1. Sélectionnez **Configuration > Réseau > Interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN que vous souhaitez supprimer. Ensuite, sélectionnez **Actions > Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

Toutes les interfaces VLAN que vous avez sélectionnées sont supprimées. Une bannière verte de succès apparaît sur la page des interfaces VLAN.

Activez StorageGRID CORS pour une interface de gestion

En tant qu'administrateur de grille, vous pouvez activer le partage de ressources entre origines (CORS) pour les requêtes d'API de gestion vers StorageGRID, si vous souhaitez que les données dans StorageGRID soient accessibles via les API de gestion à un autre domaine.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Le ["Autorisation d'accès root"](#) permet d'accéder à toutes les requêtes de configuration CORS.

À propos de cette tâche

CORS est un mécanisme de sécurité qui permet aux applications web clientes d'un domaine d'accéder aux ressources d'un autre domaine. Par exemple, supposons que vous souhaitiez créer un tableau de bord de surveillance pour StorageGRID dans le domaine `http://www.example.com`. En activant CORS dans StorageGRID pour `http://www.example.com` et « Grid Manager », le domaine StorageGRID répond aux requêtes de l'API Grid Management provenant de `http://www.example.com`.

Les requêtes Management API (mgmt-api) avec `application/json` ou `multipart/formdata` requêtes pour `Content-Type` sont prises en charge pour CORS.

Étapes

1. Dans Grid Manager, accédez à **CONFIGURATION > Réseau > Paramètres CORS de l'interface de gestion**.

2. Sélectionnez **Grid Manager**, **Tenant Manager** ou les deux options.
 - **Gestionnaire de grille** : Active CORS pour les requêtes API de gestion de grille interdomaines.
 - **Gestionnaire de locataires** : Active CORS pour les requêtes API de gestion de locataires interdomaines.
3. Saisissez l'URL de l'autre domaine dans le champ **Domains**.

Sélectionnez **Ajouter un autre domaine** si vous souhaitez activer CORS dans StorageGRID pour plus d'un domaine.

4. Sélectionnez **Enregistrer**.

Informations connexes

["Configurer StorageGRID CORS pour les compartiments et les objets"](#)

Gérer les politiques de classification du trafic

Politiques de classification du trafic dans StorageGRID

Les politiques de classification du trafic permettent d'identifier et de surveiller différents types de trafic réseau. Ces politiques peuvent faciliter la limitation et la surveillance du trafic afin d'améliorer vos offres de qualité de service (QoS).

Les politiques de classification du trafic sont appliquées aux points de terminaison du service d'équilibrage de charge StorageGRID pour les nœuds de passerelle et les nœuds d'administration. Pour créer des politiques de classification du trafic, vous devez avoir préalablement créé des points de terminaison d'équilibrage de charge.

Règles de correspondance

Chaque politique de classification du trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Compartiments
- Sous-réseau
- Locataire
- points de terminaison de l'équilibreur de charge

StorageGRID surveille le trafic correspondant à toute règle au sein de la politique, conformément aux objectifs de la règle. Tout trafic correspondant à une règle d'une politique est traité par cette politique. Inversement, vous pouvez définir des règles pour faire correspondre tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

Vous pouvez également ajouter les types de limites suivants à une politique :

- Bande passante de l'agrégat
- Bande passante par requête
- Requêtes simultanées
- Taux de requêtes

Les valeurs limites sont appliquées à chaque équilibreur de charge. Si le trafic est réparti simultanément entre plusieurs équilibreurs de charge, les débits maximaux totaux correspondent à un multiple des limites de débit que vous spécifiez.



Vous pouvez créer des règles pour limiter la bande passante de l'agrégat ou la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante de l'agrégat peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante de l'agrégat ou par requête, les requêtes sont traitées au débit que vous avez défini. StorageGRID ne peut imposer qu'une seule vitesse, donc la règle la plus spécifique, selon le type de correspondance, est celle qui est appliquée. La bande passante consommée par la requête n'est pas prise en compte dans le calcul des autres règles de correspondance moins spécifiques contenant des politiques de limite de bande passante de l'agrégat. Pour tous les autres types de limites, les requêtes client sont retardées de 250 millisecondes et reçoivent une réponse 503 Slow Down pour les requêtes qui dépassent une limite définie par une règle correspondante.

Dans le Gestionnaire de grille, vous pouvez consulter les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic attendues.

Utilisez des politiques de classification du trafic avec des SLA

Vous pouvez utiliser des politiques de classification du trafic conjointement avec des limites de capacité et la protection des données pour faire respecter des accords de niveau de service (SLA) qui précisent la capacité, la protection des données et les performances.

L'exemple suivant illustre trois niveaux d'un SLA. Vous pouvez créer des politiques de classification du trafic pour atteindre les objectifs de performance de chaque niveau de SLA.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Coût
Or	1 PB de stockage autorisé	Règle ILM 3 copies	25 K requêtes/seconde Bande passante de 5 Go/s (40 Gbit/s)	\$\$\$ par mois
Argent	250 To de stockage autorisé	Règle ILM à 2 copies	10 000 requêtes/seconde 1,25 Go/s (10 Gbit/s) de bande passante	\$\$ par mois
Bronze	100 To de stockage autorisé	Règle ILM à 2 copies	5 K requêtes/seconde Bande passante de 1 Go/s (8 Gbit/s)	\$ par mois

Vous pouvez créer des politiques de classification du trafic si vous souhaitez surveiller et, éventuellement, limiter le trafic réseau par compartiment, expression régulière de compartiment, CIDR, point de terminaison d'équilibreur de charge ou locataire. Vous pouvez également définir des limites pour une politique en fonction de la bande passante, du nombre de requêtes simultanées ou du débit de requêtes.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Vous avez créé tous les points de terminaison de load balancer que vous souhaitez faire correspondre.
- Vous avez créé tous les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.
2. Sélectionnez **Create**.
3. Saisissez un nom et une description (facultatif) pour la règle, puis sélectionnez **Continuer**.

Par exemple, décrivez à quoi s'applique cette politique de classification du trafic et ce qu'elle limitera.

4. Sélectionnez **Ajouter une règle** et indiquez les détails suivants pour créer une ou plusieurs règles correspondant à la stratégie. Toute stratégie que vous créez doit comporter au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels s'applique la règle de correspondance. Les types de trafic sont : bucket, expression régulière de bucket, CIDR, point de terminaison de load balancer et tenant.

Champ	Description
Valeur de correspondance	Saisissez la valeur correspondant au type sélectionné. • Compartiment : Saisissez un ou plusieurs noms de compartiment. • Expression régulière pour les compartiments : saisissez une ou plusieurs expressions régulières utilisées pour faire correspondre un ensemble de noms de compartiments. L'expression régulière n'est pas ancrée. Utilisez l'ancrage ^ pour effectuer une correspondance au début du nom du compartiment, et l'ancrage \$ pour effectuer une correspondance à la fin du nom. La correspondance par expression régulière prend en charge un sous-ensemble de la syntaxe PCRE (Perl compatible regular expression). • CIDR : Entrez un ou plusieurs sous-réseaux IPv4, en notation CIDR, qui correspondent au sous-réseau souhaité. • Point de terminaison de l'équilibreur de charge : sélectionnez un nom de point de terminaison. Voici les points de terminaison de l'équilibreur de charge que vous avez définis sur le "Configurer les points de terminaison de l'équilibreur de charge". • Locataire : L'identification du locataire repose sur l'identifiant de clé d'accès. Si la requête ne contient pas d'identifiant de clé d'accès (par exemple, accès anonyme), alors la propriété du compartiment consulté est utilisée pour déterminer le locataire.
Correspondance inverse	Si vous souhaitez faire correspondre tout le trafic réseau <i>à l'exception</i> du trafic conforme au Type et à la valeur de correspondance que vous venez de définir, cochez la case Correspondance inverse. Sinon, laissez la case décochée. Par exemple, si vous souhaitez que cette politique s'applique à tous les points de terminaison de l'équilibreur de charge sauf un, spécifiez le point de terminaison de l'équilibreur de charge à exclure et sélectionnez Correspondance inverse. Pour une politique contenant plusieurs critères de correspondance, dont au moins un est un critère de correspondance inverse, veillez à ne pas créer une politique qui correspond à toutes les requêtes.

5. Vous pouvez également sélectionner **Ajouter une limite** et sélectionner les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.



StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez comprendre les tendances du trafic.

Champ	Description
Type	Le type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le débit de requêtes. Remarque : Vous pouvez créer des règles pour limiter la bande passante de l'agrégat ou la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante de l'agrégat est utilisée, la bande passante par requête est indisponible. Inversement, lorsque la bande passante par requête est utilisée, la bande passante de l'agrégat est indisponible. Les limites de la bande passante de l'agrégat peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la règle la plus adaptée au type de limite défini. Par exemple, si vous avez une règle qui limite le trafic dans un seul sens, alors le trafic dans le sens opposé sera illimité, même s'il existe du trafic correspondant à d'autres règles imposant des limites de bande passante. StorageGRID applique les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (masque /32) • Nom exact du compartiment • Expression régulière de compartiment • Locataire • Point de terminaison • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Que cette limite s'applique aux requêtes de lecture du client (GET ou HEAD) ou aux requêtes d'écriture (PUT, POST ou DELETE).
Valeur	La valeur à laquelle le trafic réseau sera limité, en fonction de l'unité que vous sélectionnez. Par exemple, saisissez 10 et sélectionnez Mio/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. Remarque : Selon le paramètre d'unités, les unités disponibles seront binaires (par exemple, GiB) ou décimales (par exemple, GB). Pour modifier le paramètre d'unités, sélectionnez le menu déroulant utilisateur en haut à droite du Grid Manager, puis sélectionnez User Preferences.
Unité	L'unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de l'agrégat de 4 Go/s pour un niveau SLA, créez deux limites de bande passante de l'agrégat : GET/HEAD à 4 Go/s et PUT/POST/DELETE à 4 Go/s.

6. Sélectionnez **Continue**.

7. Veuillez lire et examiner la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la politique, sélectionnez **Enregistrer et continuer**.

Le trafic client S3 est désormais géré conformément à la politique de classification du trafic.

Après avoir terminé

"Afficher les indicateurs de trafic réseau" pour vérifier que les règles appliquent les limites de trafic que vous attendez.

Modifier une politique de classification du trafic StorageGRID

Vous pouvez modifier une politique de classification du trafic pour en changer le nom ou la description, ou pour créer, modifier ou supprimer des règles ou des limites pour cette politique.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page des politiques de classification du trafic s'affiche et les politiques existantes sont répertoriées dans un tableau.

2. Modifiez la politique via le menu Actions ou la page de détails. Consultez "créer des politiques de classification du trafic" pour savoir quoi saisir.

Menu Actions

- a. Cochez la case correspondant à la politique.
- b. Sélectionnez **Actions > Modifier**.

Page de détails

- a. Sélectionnez le nom de la règle.
- b. Sélectionnez le bouton **Modifier** situé à côté du nom de la stratégie.

3. À l'étape « Saisir le nom de la politique », vous pouvez éventuellement modifier le nom ou la description de la politique, puis sélectionner **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, vous pouvez éventuellement ajouter une règle ou modifier le **Type** et la **valeur de correspondance** de la règle existante, puis sélectionner **Continuer**.
5. À l'étape Définir les limites, vous pouvez éventuellement ajouter, modifier ou supprimer une limite, puis sélectionner **Continuer**.
6. Examinez la politique mise à jour, puis sélectionnez **Enregistrer et continuer**.

Les modifications apportées à la politique ont été enregistrées et le trafic réseau est désormais géré conformément aux politiques de classification du trafic. Vous pouvez consulter les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic que vous attendez.

Supprimer une politique de classification du trafic StorageGRID

Vous pouvez supprimer une règle de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la bonne règle, car une règle ne peut pas être récupérée une fois supprimée.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page des politiques de classification du trafic affiche les politiques existantes répertoriées dans un tableau.

2. Supprimez la politique à l'aide du menu Actions ou de la page de détails.

Menu Actions

- a. Cochez la case correspondant à la politique.
- b. Sélectionnez **Actions > Supprimer**.

Page de détails de la politique

- a. Sélectionnez le nom de la règle.
- b. Sélectionnez le bouton **Supprimer** situé à côté du nom de la stratégie.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la politique.

La politique a été supprimée.

Afficher les indicateurs de trafic réseau dans StorageGRID

Vous pouvez surveiller le trafic réseau en consultant les graphiques disponibles sur la page des politiques de classification du trafic.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root ou autorisation de comptes locataires"](#).

À propos de cette tâche

Pour toute politique de classification du trafic existante, vous pouvez consulter les indicateurs du service de load balancer afin de déterminer si la politique limite efficacement le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la politique.

Même si aucune limite n'est fixée pour une politique de classification du trafic, des indicateurs sont collectés et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.

La page des politiques de classification du trafic s'affiche et les politiques existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la politique de classification du trafic pour laquelle vous souhaitez consulter les indicateurs.

3. Sélectionnez l'onglet **Métriques**.

Les graphiques de la politique de classification du trafic s'affichent. Les graphiques présentent des indicateurs uniquement pour le trafic correspondant à la politique sélectionnée.

Les graphiques suivants figurent sur la page.

- Débit des requêtes : ce graphique indique la quantité de bande passante correspondant à cette politique, gérée par l'ensemble des équilibres de charge. Les données reçues comprennent les en-têtes de toutes les requêtes et la taille du corps des réponses qui contiennent des données de corps. Les données envoyées comprennent les en-têtes de réponse pour toutes les requêtes et la taille du corps de la réponse pour les requêtes qui incluent des données de corps dans la réponse.



Une fois les requêtes terminées, ce graphique affiche uniquement l'utilisation de la bande passante. Pour les requêtes lentes ou portant sur des objets volumineux, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

- Taux de réponse en cas d'erreur : ce graphique fournit un taux approximatif auquel les requêtes correspondant à cette politique renvoient des erreurs (code d'état HTTP ≥ 400) aux clients.
 - Durée moyenne des requêtes (sans erreur) : ce graphique présente la durée moyenne des requêtes réussies correspondant à cette politique.
 - Utilisation de la bande passante de la politique : ce graphique indique la quantité de bande passante correspondant à cette politique, gérée par l'ensemble des équilibres de charge. Les données reçues comprennent les en-têtes de requête pour toutes les requêtes et la taille des données du corps pour les réponses qui en contiennent. Les données envoyées comprennent les en-têtes de réponse pour toutes les requêtes et la taille des données du corps de la réponse pour les requêtes dont la réponse contient des données de corps.
4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle des valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Grafana dashboard** juste en dessous du titre **Metrics** pour afficher tous les graphiques d'une policy. En plus des quatre graphiques de l'onglet **Metrics**, vous pouvez en consulter deux autres :
- Taux de requêtes d'écriture par taille d'objet : Ce taux correspond aux requêtes PUT/POST/DELETE conformes à cette politique. Le positionnement sur une cellule indique le taux par seconde. Les taux affichés au survol sont tronqués à un nombre entier et peuvent indiquer 0 même lorsqu'il y a des requêtes non nulles dans le compartiment.
 - Taux de requêtes de lecture par taille d'objet : le taux des requêtes GET/HEAD correspondant à cette politique. Le positionnement sur une cellule individuelle indique les taux par seconde. Les taux affichés au survol sont tronqués à des nombres entiers et peuvent indiquer 0 même s'il y a des requêtes non nulles dans le compartiment.
6. Vous pouvez également accéder aux graphiques depuis le menu **Support**.
- a. Sélectionnez **Support > Tools > Metrics**.

- b. Sélectionnez **Politique de classification du trafic** dans la section **Grafana**.
- c. Sélectionnez la règle dans le menu situé en haut à gauche de la page.
- d. Placez le curseur sur un graphique pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles des objets agrégées dans le décompte et le nombre de requêtes par seconde pendant cette période.

Les politiques de classification du trafic sont identifiées par leur identifiant. Les identifiants des politiques sont répertoriés sur la page des politiques de classification du trafic.

7. Analysez les graphiques pour déterminer la fréquence à laquelle la politique limite le trafic et si vous devez ajuster la politique.

Chiffrements pris en charge pour les connexions TLS sortantes dans StorageGRID

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (Transport Layer Security) aux systèmes externes utilisés pour la fédération d'identité et les Cloud Storage Pools.

Versions de TLS prises en charge

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération d'identité et les Cloud Storage Pools.

Les suites de chiffrement TLS prises en charge pour les systèmes externes ont été sélectionnées afin de garantir la compatibilité avec un large éventail de systèmes externes. La liste est plus longue que la liste des suites de chiffrement prises en charge pour les applications clientes S3. Pour configurer les suites de chiffrement, allez dans **Configuration > Sécurité > Paramètres de sécurité** et sélectionnez **Stratégies TLS et SSH**.



Les options de configuration TLS, telles que les versions de protocole, les algorithmes de chiffrement, les algorithmes d'échange de clés et les algorithmes MAC, ne sont pas configurables dans StorageGRID. Contactez votre représentant de compte NetApp si vous avez des demandes spécifiques concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées dans StorageGRID

La façon dont vous configurez les connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations diffèrent selon que la connexion HTTP est active, inactive ou si vous avez plusieurs connexions simultanées.

Vous pouvez identifier les gains de performance pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages du maintien des connexions HTTP inactives ouvertes

Maintenez les connexions HTTP ouvertes lorsque les applications clientes sont inactives afin de permettre des transactions ultérieures. Maintenez une connexion HTTP inactive ouverte pendant un maximum de 10 minutes. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive

pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Latence réduite entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut l'exécuter

La réduction de la latence est le principal avantage, notamment en ce qui concerne le temps nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation du débit de transfert des données grâce à l'amorçage de l'algorithme de démarrage lent TCP/IP avec des transferts précédemment effectués
- Notification instantanée de plusieurs types de pannes interrompant la connectivité entre l'application cliente et le système StorageGRID

Déterminez la durée de maintien d'une connexion inactive en équilibrant les avantages d'un démarrage lent et l'allocation des ressources.

Avantages des connexions HTTP actives

Pour les connexions directes aux nœuds de stockage, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue des transactions en continu.

Déterminer la durée maximale pendant laquelle une connexion doit être maintenue ouverte implique un compromis entre les avantages de la persistance de la connexion et l'allocation idéale de la connexion aux ressources internes du système.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Permet un équilibrage de charge optimal sur l'ensemble du système StorageGRID.

Avec le temps, une connexion HTTP peut ne plus être optimale à mesure que les exigences en matière d'équilibrage de charge évoluent. Le système offre son meilleur équilibrage de charge lorsque les applications clientes établissent une connexion HTTP distincte pour chaque transaction, mais cette méthode annule les gains précieux associés aux connexions persistantes.

- Permet aux applications clientes de diriger les transactions HTTP vers les services LDR disposant d'espace disponible.
- Permet de lancer les procédures de maintenance.

Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service de Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre à certaines procédures de maintenance de démarrer rapidement. Si la durée des connexions client n'est pas limitée, il peut s'écouler plusieurs minutes avant que les connexions actives ne soient automatiquement fermées.

Avantages des connexions HTTP simultanées

Il est conseillé de maintenir plusieurs connexions TCP/IP ouvertes vers le système StorageGRID afin de permettre le traitement parallèle, ce qui améliore les performances. Le nombre optimal de connexions parallèles dépend de plusieurs facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

Les transactions peuvent démarrer immédiatement au lieu d'attendre que d'autres transactions soient terminées.

- Débit accru

Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit de transactions agrégé.

Les applications clientes doivent établir plusieurs connexions HTTP. Lorsqu'une application cliente doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui n'est pas en train de traiter une transaction.

La topologie de chaque système StorageGRID présente un débit de pointe différent pour les transactions et connexions simultanées. Le débit de pointe dépend des ressources de calcul, de réseau, de stockage, des liaisons WAN, ainsi que du nombre de serveurs, de services et d'applications que le système StorageGRID prend en charge.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications clientes. Tenez-en compte lorsque vous déterminez le nombre maximal de connexions simultanées. Si l'application cliente est composée de plusieurs entités logicielles qui établissent chacune des connexions au système StorageGRID, additionnez toutes les connexions de ces entités. Vous devrez peut-être ajuster le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID influe sur le nombre maximal de transactions et de connexions simultanées que le système peut prendre en charge.
- Les applications clientes qui interagissent avec le système StorageGRID sur un réseau à bande passante limitée peuvent devoir réduire leur niveau de concurrence afin de garantir que chaque transaction soit effectuée dans un délai raisonnable.
- Lorsque de nombreuses applications clientes partagent le système StorageGRID, vous devrez peut-être réduire le degré de concurrence afin d'éviter de dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools distincts de connexions HTTP pour les opérations de lecture et d'écriture et contrôler la part de chaque pool à utiliser pour chacune. Des pools distincts de connexions HTTP vous permettent de mieux contrôler les transactions et d'équilibrer les charges.

Les applications clientes peuvent générer des charges à dominante récupération (lecture) ou à dominante stockage (écriture). Avec des pools distincts de connexions HTTP pour les transactions de lecture et d'écriture, vous pouvez ajuster la part de chaque pool à consacrer aux transactions de lecture ou d'écriture.

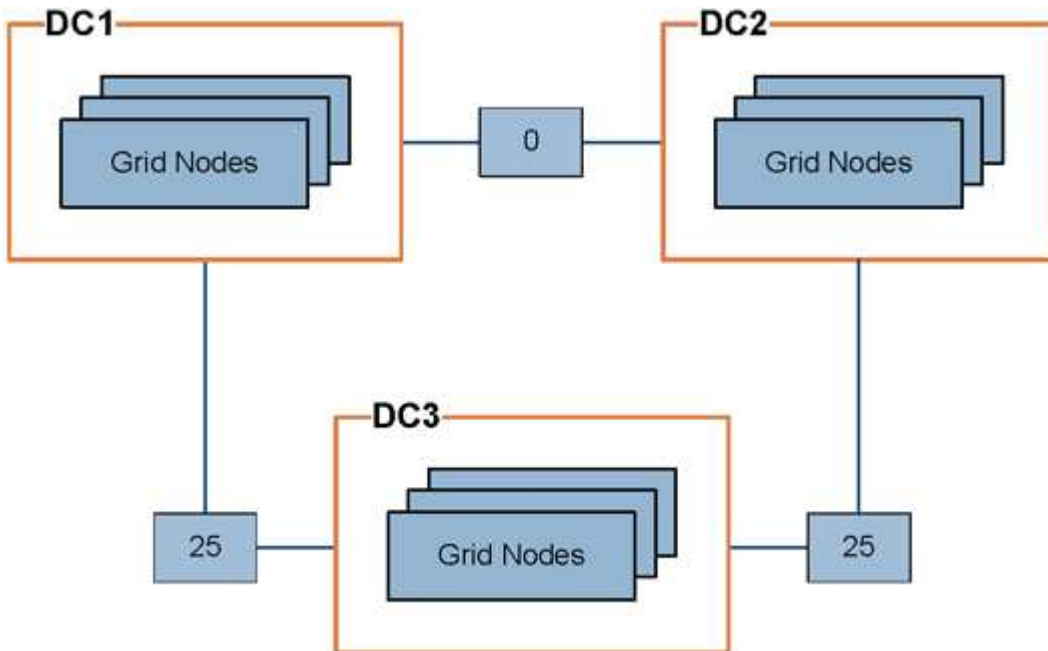
Gérer les coûts de liaison dans StorageGRID

Les coûts des liens vous permettent de prioriser le site de centre de données qui fournit un service demandé lorsque deux sites de centre de données ou plus existent. Vous pouvez ajuster les coûts des liens pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts des liens servent à déterminer quelle copie d'objet est utilisée pour effectuer les récupérations d'objet.
- Les coûts de liaison sont utilisés par l'API de gestion de la grille et l'API de gestion des locataires pour déterminer quels services internes StorageGRID utiliser.
- Le service d'équilibrage de charge utilise les coûts de liaison sur les nœuds d'administration et les nœuds de passerelle pour diriger les connexions client. Voir "[Considérations relatives à l'équilibrage de charge](#)".

Le diagramme montre une grille à trois sites avec des coûts de liaison configurés entre les sites :



- Le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle répartit équitablement les connexions clientes entre tous les nœuds de stockage du même site de centre de données et tous les sites de centre de données dont le coût de liaison est de 0.

Dans cet exemple, un nœud de passerelle du site de centre de données 1 (DC1) répartit équitablement les connexions client entre les nœuds de stockage de DC1 et les nœuds de stockage de DC2. Un nœud de passerelle de DC3 envoie les connexions client uniquement aux nœuds de stockage de DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie située dans le centre de données dont le coût de liaison est le plus faible.

Dans l'exemple, si une application cliente à DC2 récupère un objet qui est stocké à la fois à DC1 et à DC3, l'objet est récupéré depuis DC1, car le coût de liaison de DC1 à DC2 est de 0, ce qui est inférieur au coût de liaison de DC3 à DC2 (25).

Les coûts de liaison sont des valeurs relatives arbitraires sans unité de mesure spécifique. Par exemple, un coût de liaison de 50 est utilisé moins préférentiellement qu'un coût de 25. Le tableau présente les coûts de liaison les plus couramment utilisés.

Lien	Coût de liaison	Remarques
Entre les sites physiques des centres de données	25 (par défaut)	Centres de données connectés par une liaison WAN.
Entre sites de centres de données logiques situés au même emplacement physique	0	Centres de données logiques dans le même bâtiment ou campus physique connectés par un LAN.

Mettre à jour les coûts des liens

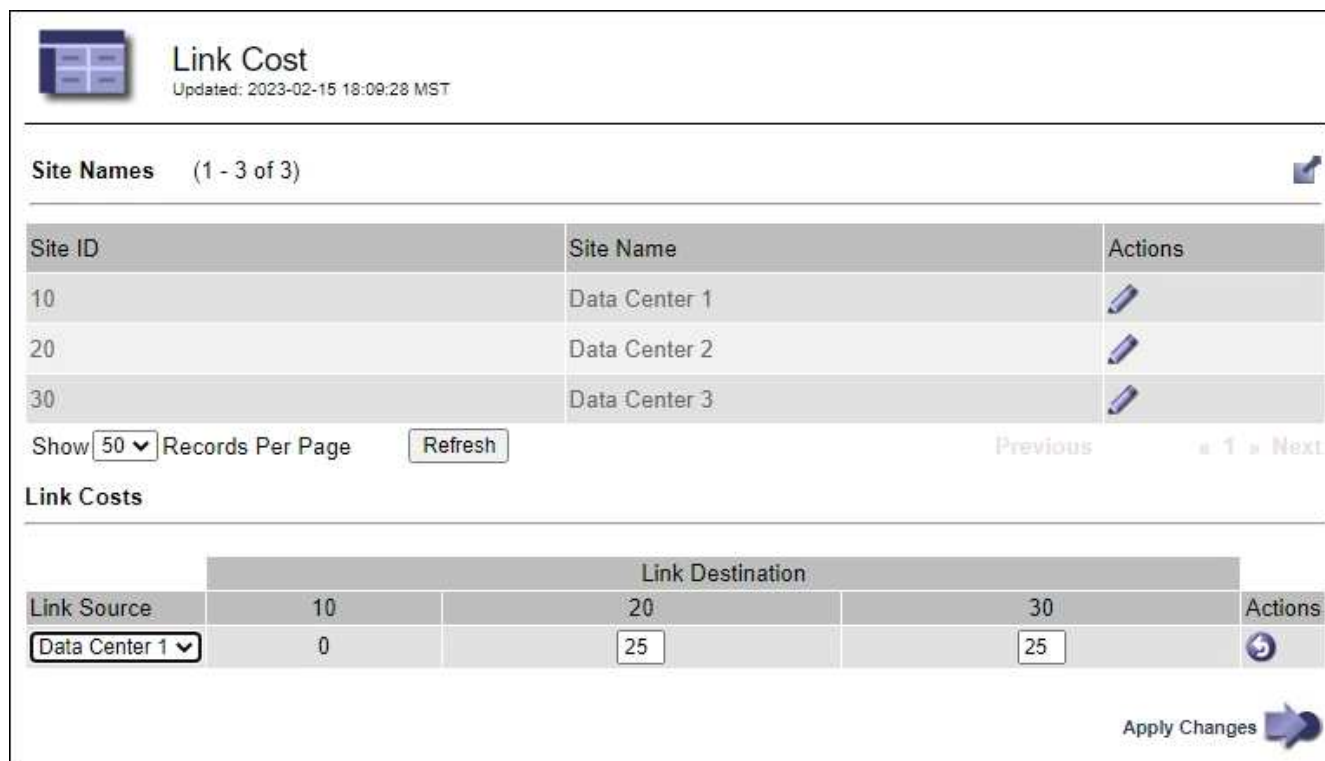
Vous pouvez mettre à jour les coûts de liaison entre les sites de centres de données pour refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autre autorisation de configuration de grille"](#).

Étapes

1. Sélectionnez **Support > Other > Link cost**.



Link Cost
Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page Previous 1 Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	

2. Sélectionnez un site sous **Source du lien** et saisissez une valeur de coût entre 0 et 100 sous **Destination du lien**.

Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

Pour annuler les modifications, sélectionnez **Revert**.

3. Sélectionnez **Appliquer les modifications**.

Utilisez AutoSupport

Découvrez AutoSupport dans StorageGRID

La fonctionnalité AutoSupport permet à StorageGRID d'envoyer des rapports d'état et de santé à l'assistance technique NetApp.

L'utilisation de AutoSupport aide à résoudre les problèmes plus rapidement. L'assistance technique peut surveiller les besoins de stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. En option, AutoSupport peut envoyer des paquets vers une destination supplémentaire.

StorageGRID propose deux types de AutoSupport :

- **StorageGRID AutoSupport** signale les problèmes logiciels de StorageGRID. Activé par défaut lors de la première installation de StorageGRID. Vous pouvez ["modifiez la configuration AutoSupport par défaut"](#) si nécessaire.



Si StorageGRID AutoSupport n'est pas activé, un message s'affiche sur le tableau de bord du Grid Manager. Le message inclut un lien vers la page de configuration AutoSupport. Si vous fermez le message, il ne s'affichera plus tant que le cache de votre navigateur n'aura pas été vidé, même si AutoSupport reste désactivé.

- **Le matériel de l'appliance AutoSupport** signale des problèmes avec l'appliance StorageGRID. Vous devez ["configurer le matériel AutoSupport sur chaque appareil"](#).

Qu'est-ce que Active IQ ?

Active IQ est un conseiller numérique basé sur le cloud qui exploite l'analyse prédictive et l'expertise de la base installée de NetApp. Ses évaluations continues des risques, ses alertes prédictives, ses recommandations prescriptives et ses actions automatisées vous aident à prévenir les problèmes avant qu'ils ne surviennent, ce qui améliore la santé du système et augmente la disponibilité du système.

Si vous souhaitez utiliser les tableaux de bord et la fonctionnalité Active IQ sur le site d'assistance NetApp, vous devez activer AutoSupport.

["Documentation Active IQ Digital Advisor"](#)

Informations incluses dans le package AutoSupport

Un paquet AutoSupport contient les fichiers et détails suivants.

Nom des fichiers	Champs	Description
AUTOSUPPORT-HISTORY.XML	AutoSupport Sequence Number + Destination for this AutoSupport + Statut de la livraison + Tentatives de livraison + AutoSupport Sujet + URI de livraison + Dernière erreur + AutoSupport PUT Nom du fichier + Heure de génération + Taille compressée Autosupport + Taille décompressée Autosupport + Durée totale de collecte (ms)	AutoSupport fichier historique.
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + Adresse de support + AutoSupport OnDemand État + AutoSupport OnDemand Server URL + AutoSupport OnDemand Polling Interval	Fichier d'état AutoSupport. Fournit des détails sur le protocole utilisé, l'URL et l'adresse du support technique, l'intervalle d'interrogation, et si OnDemand AutoSupport est activé ou désactivé.
BUCKETS.XML	ID du compartiment + ID du compte + Version de la build + Configuration des contraintes d'emplacement + Conformité activée + Configuration de la conformité + Verrouillage des objets S3 activé + Configuration du verrouillage des objets S3 + Configuration de la cohérence + CORS activé + Configuration CORS + Heure du dernier accès activée + Stratégie activée + Configuration de la stratégie + Notifications activées + Configuration des notifications + Cloud Mirror activé + Configuration de Cloud Mirror + Recherche activée + Configuration de la recherche + Étiquetage des compartiments activé + Configuration de l'étiquetage des compartiments + Configuration du versionnage	Fournit des détails de configuration et des statistiques au niveau du compartiment. Les configurations de compartiment incluent par exemple les services de plateforme, la conformité et la cohérence du compartiment.

Nom des fichiers	Champs	Description
GRID-CONFIGURATIONS.XML	ID de l'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations de configuration à l'échelle de la grille. Contient des informations sur les certificats de la grille, l'espace réservé aux métadonnées, les paramètres de configuration à l'échelle de la grille (conformité, S3 Object Lock, compression d'objets, alertes, syslog et configuration ILM), les détails du profil de codage d'effacement, le nom DNS et "Nom NMS".
GRID-SPEC.XML	Spécifications de la grille, XML brut	Utilisé pour configurer et déployer StorageGRID. Contient les spécifications de la grille, l'adresse IP du serveur NTP, l'adresse IP du serveur DNS, la topologie du réseau et les profils matériels des nœuds.
GRID-TASKS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'état des tâches de la grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, achevées, ayant échoué et en attente de la grille.
GRID.JSON	Grille + Révision + Version du logiciel + Description + Licence + Mots de passe + DNS + NTP + Sites + Nœuds	Informations sur la grille.
ILM-CONFIGURATION.XML	ID de l'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Liste des attributs des configurations ILM.
ILM-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations sur les métriques ILM. Contient les taux d'évaluation ILM pour chaque nœud et les métriques à l'échelle de la grille.
ILM.XML	XML brut ILM	Fichier de stratégie ILM active. Contient des informations détaillées sur les stratégies ILM actives, telles que l'ID du pool de stockage, le comportement d'ingestion, les filtres, les règles et la description.
LOG.TGZ	<i>n/a</i>	Fichier journal téléchargeable. Contient <code>broadcast-err.log</code> et <code>servermanager.log</code> de chaque nœud.

Nom des fichiers	Champs	Description
MANIFEST.XML	Ordre de collecte + AutoSupport nom de fichier de contenu pour ces données + description de cet élément de données + nombre d'octets collectés + temps passé à collecter + statut de cet élément de données + description de l'erreur + AutoSupport type de contenu pour ces données +	Contient les métadonnées AutoSupport et de brèves descriptions de tous les fichiers AutoSupport.
NMS-ENTITIES.XML	Index d'attribut + OID d'entité + ID de nœud + ID de modèle de périphérique + Version de modèle de périphérique + Nom de l'entité	Les entités de groupe et de service dans le "Arbre NMS". Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.
OBJECTS-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	État des objets, y compris l'état de l'analyse en arrière-plan, le transfert actif, le taux de transfert, le nombre total de transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la réparation tentée, le taux d'analyse, la période d'analyse estimée et l'état d'achèvement de la réparation.
SERVER-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Configurations du serveur. Contient les détails suivants pour chaque nœud : type de plateforme, système d'exploitation, mémoire installée, mémoire disponible, connectivité de stockage, numéro de série du châssis de l'apppliance de stockage, nombre de disques défaillants du contrôleur de stockage, température du châssis du contrôleur de calcul, matériel de calcul, numéro de série du contrôleur de calcul, alimentation électrique, taille du disque et type de disque.
SERVICE-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations du nœud de service. Contient des détails tels que l'espace de table alloué, l'espace de table libre, les métriques Reaper de la base de données, la durée de réparation des segments, la durée des tâches de réparation, les redémarrages automatiques des tâches et l'arrêt automatique des tâches.

Nom des fichiers	Champs	Description
STORAGE-GRADES.XML	ID de niveau de stockage + Nom de niveau de stockage + ID du nœud de stockage + Chemin du nœud de stockage	Fichier de définitions de qualité de stockage pour chaque nœud de stockage.
SUMMARY-ATTRIBUTES.XML	OID du groupe + Chemin du groupe + ID de l'attribut de synthèse + Nom de l'attribut de synthèse + Valeur + Index + ID de la table + Nom de la table	Données d'état système de haut niveau récapitulant les informations d'utilisation de StorageGRID. Fournit des détails tels que le nom de la grille, les noms des sites, le nombre de nœuds de stockage par grille et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions de support logiciel et les détails des opérations S3.
SYSTEM-ALERTS.XML	Nom + Gravité + Nom du nœud + Statut de l'alerte + Nom du site + Heure de déclenchement de l'alerte + Heure de résolution de l'alerte + ID de la règle + ID du nœud + ID du site + Désactivé + Autres annotations + Autres étiquettes	Alertes système actuelles indiquant des problèmes potentiels dans le système StorageGRID.
USERAGENTS.XML	Agent utilisateur + Nombre de jours + Nombre total de requêtes HTTP + Nombre total d'octets ingérés + Nombre total d'octets récupérés + Requêtes PUT + Requêtes GET + Requêtes DELETE + Requêtes HEAD + Requêtes POST + Requêtes OPTIONS + Temps moyen de requête (ms) + Temps moyen de requête PUT (ms) + Temps moyen de requête GET (ms) + Temps moyen de requête DELETE (ms) + Temps moyen de requête HEAD (ms) + Temps moyen de requête POST (ms) + Temps moyen de requête OPTIONS (ms)	Statistiques basées sur les agents utilisateurs de l'application. Par exemple, le nombre d'opérations PUT/GET/DELETE/HEAD par agent utilisateur et la taille totale en octets de chaque opération.

Nom des fichiers	Champs	Description
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	AutoSupport Données d'en-tête.

Configurer AutoSupport dans StorageGRID

Par défaut, la fonctionnalité AutoSupport de StorageGRID est activée lors de la première installation de StorageGRID. Cependant, vous devez configurer le AutoSupport matériel sur chaque appliance. Au besoin, vous pouvez modifier la configuration AutoSupport.

Si vous souhaitez modifier la configuration de StorageGRID AutoSupport, effectuez vos modifications uniquement sur le nœud d'administration principal. Vous devez [configurer le matériel AutoSupport](#) sur chaque appliance.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Si vous utilisez HTTPS pour l'envoi de colis AutoSupport, vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit ["utilisation d'un serveur proxy"](#) (les connexions entrantes ne sont pas requises).
- Si HTTP est sélectionné sur la page StorageGRID AutoSupport, vous devez ["configuré un serveur proxy"](#) pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejeteront les packages envoyés via HTTP.
- Si vous utilisez SMTP comme protocole pour les paquets AutoSupport, vous avez configuré un serveur de messagerie SMTP.

À propos de cette tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire** : Envoyez automatiquement les packages AutoSupport une fois par semaine. Paramètre par défaut : Activé.
- **Déclenchement par événement** : Envoyez automatiquement des paquets AutoSupport toutes les heures ou lors d'événements système importants. Paramètre par défaut : Activé.
- **À la demande** : Autorise le support technique à demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport, ce qui est utile lorsqu'ils traitent activement un problème (nécessite le protocole de transmission AutoSupport en HTTPS). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : Envoyez manuellement des packages AutoSupport à tout moment.
- **Collecte des journaux** : ["Collecter manuellement les fichiers journaux et les données système et envoyer un colis AutoSupport"](#).

Spécifiez le protocole pour les paquets AutoSupport

Vous pouvez utiliser l'un des protocoles suivants pour envoyer des packages AutoSupport :

- **HTTPS** : Il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Ce protocole utilise le port 443. Si vous souhaitez [activer la fonction AutoSupport on Demand](#), vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejettent les packages envoyés via HTTP. Ce protocole utilise le port 80.
- **SMTP** : Utilisez cette option si vous souhaitez que les packages AutoSupport soient envoyés par e-mail.

Le protocole que vous avez défini est utilisé pour l'envoi de tous les types de packages AutoSupport.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.
2. Sélectionnez le protocole que vous souhaitez utiliser pour envoyer des paquets AutoSupport.
3. Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat de support NetApp (certificat TLS) pour sécuriser la connexion au serveur de support technique.
 - **Vérifier le certificat** (par défaut) : Garantit que la transmission des paquets AutoSupport est sécurisée. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
 - **Ne pas vérifier le certificat** : Sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation du certificat, par exemple en cas de problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**. Tous les paquets hebdomadaires, déclenchés par l'utilisateur et déclenchés par un événement, sont envoyés en utilisant le protocole sélectionné.

Désactiver l'envoi hebdomadaire AutoSupport

Par défaut, le système StorageGRID est configuré pour envoyer un AutoSupport package au support technique une fois par semaine.

Pour déterminer quand le package hebdomadaire AutoSupport sera envoyé, allez dans l'onglet **AutoSupport > Results**. Dans la section **Weekly AutoSupport**, regardez la valeur de **Next Scheduled Time**.

Vous pouvez désactiver l'envoi automatique des packages hebdomadaires AutoSupport à tout moment.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.
2. Décochez la case **Activer l'AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactiver le déclenchement par événement AutoSupport

Par défaut, le système StorageGRID est configuré pour envoyer un paquet AutoSupport au support technique toutes les heures.

Vous pouvez désactiver le déclenchement par événement AutoSupport à tout moment.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.

2. Décochez la case **Activer le déclenchement par événement AutoSupport**.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport à la demande

AutoSupport on Demand peut aider à résoudre les problèmes sur lesquels le support technique travaille activement.

Par défaut, AutoSupport on Demand est désactivé. L'activation de cette fonctionnalité permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport. Le support technique peut également définir l'intervalle de temps d'interrogation pour les requêtes AutoSupport on Demand.

L'assistance technique ne peut pas activer ou désactiver AutoSupport on Demand.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.
2. Sélectionnez **HTTPS** pour le protocole.
3. Cochez la case **Activer l'hebdomadaire AutoSupport**.
4. Cochez la case **Activer AutoSupport à la demande**.
5. Sélectionnez **Enregistrer**.

AutoSupport on Demand est activé, et le support technique peut envoyer des requêtes AutoSupport on Demand à StorageGRID.

Désactiver la vérification 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 de mise à niveau StorageGRID.

Si nécessaire, vous pouvez désactiver la vérification des mises à jour logicielles. Par exemple, si votre système n'a pas d'accès WAN, vous devez désactiver la vérification afin d'éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.
2. Décochez la case **Rechercher les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les paquets de santé et d'état sont envoyés au support technique. Vous pouvez spécifier une destination supplémentaire pour tous les paquets AutoSupport.

Pour vérifier ou modifier le protocole utilisé pour envoyer des paquets AutoSupport, consultez les instructions à [spécifier le protocole pour les paquets AutoSupport](#).



Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des paquets AutoSupport vers une destination supplémentaire.

Étapes

1. Sélectionnez **Support > Outils > AutoSupport > Paramètres**.
2. Sélectionnez **Activer une destination AutoSupport supplémentaire**.
3. Spécifiez les éléments suivants :

Nom d'hôte

Le nom d'hôte ou l'adresse IP d'un serveur de destination AutoSupport supplémentaire.



Vous ne pouvez saisir qu'une seule destination supplémentaire.

Port

Le port utilisé pour se connecter à un serveur de destination AutoSupport supplémentaire. La valeur par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS.

Validation du certificat

Indique si un certificat TLS est utilisé pour sécuriser la connexion à la destination supplémentaire.

- Sélectionnez **Vérifier le certificat** pour utiliser la validation du certificat.
- Sélectionnez **Ne pas vérifier le certificat** pour envoyer vos AutoSupport packages sans validation de certificat.

Ne choisissez cette option que si vous avez une bonne raison de ne pas utiliser la validation des certificats, par exemple en cas de problème temporaire avec un certificat.

4. Si vous avez sélectionné **Vérifier le certificat**, procédez comme suit :
 - a. Accédez à l'emplacement du certificat CA.
 - b. Téléversez le fichier de certificat de l'autorité de certification.

Les métadonnées du certificat d'autorité de certification apparaissent.

5. Sélectionnez **Enregistrer**.

Tous les futurs colis AutoSupport hebdomadaires, déclenchés par des événements ou par l'utilisateur, seront envoyés à la destination supplémentaire.

Configurer AutoSupport pour les appareils

AutoSupport pour les appliances signale les problèmes matériels StorageGRID, et StorageGRID AutoSupport signale les problèmes logiciels StorageGRID, à une exception près : pour le SGF6112, StorageGRID AutoSupport signale à la fois les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appliance, sauf le SGF6112 qui ne nécessite aucune configuration supplémentaire. AutoSupport est mis en œuvre différemment pour les appliances de services et les appliances de stockage.

Vous utilisez SANtricity pour activer AutoSupport pour chaque appliance de stockage. Vous pouvez configurer SANtricity AutoSupport lors de la configuration initiale de l'appliance ou après l'installation d'une appliance :

- Pour les appareils SG6000 et SG5700, "[configurer AutoSupport dans SANtricity System Manager](#)"

AutoSupport packages des appliances E-Series peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans "[SANtricity System Manager](#)".

StorageGRID AutoSupport ne signale pas les problèmes matériels, tels que les défaillances des modules DIMM ou des cartes d'interface d'hôte (HIC). Cependant, certaines pannes de composants peuvent déclencher "[alertes matérielles](#)". Pour les appliances StorageGRID équipées d'un contrôleur de gestion de carte mère (BMC), vous pouvez configurer l'envoi d'e-mails et de traps SNMP pour signaler les pannes matérielles.

- "[Configurer les notifications par e-mail pour les alertes BMC](#)"
- "[Configurer les paramètres SNMP pour BMC](#)"

Informations connexes

["Support NetApp"](#)

Déclencher manuellement un AutoSupport package dans StorageGRID

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un package AutoSupport.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous disposez de l'accès racine ou de l'autorisation de configuration de grille.

Étapes

1. Sélectionnez **Support > Tools > AutoSupport**.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenché par l'utilisateur**.

StorageGRID tente d'envoyer un paquet AutoSupport au site de support NetApp. En cas de succès, les valeurs **Résultat le plus récent** et **Dernière tentative réussie** de l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** passe à « Échec », et StorageGRID n'essaie pas de renvoyer le paquet AutoSupport.

3. Au bout d'une minute, actualisez la page AutoSupport dans votre navigateur pour accéder aux résultats les plus récents.



De plus, vous pouvez "[collecter des fichiers journaux et des données système plus étendus](#)" et les envoyer au site d'assistance NetApp.

Dépanner les packages AutoSupport de StorageGRID

Si une tentative d'envoi d'un package AutoSupport échoue, le système StorageGRID prend différentes mesures selon le type de package AutoSupport. Vous pouvez vérifier l'état des packages AutoSupport en sélectionnant **Support > Outils > AutoSupport > Résultats**.

Lorsque le package AutoSupport ne parvient pas à être envoyé, « Échec » apparaît dans l'onglet **Résultats** de la page **AutoSupport**.



Si vous avez configuré un serveur proxy pour transférer les paquets AutoSupport à NetApp, vous devriez "[vérifier que les paramètres de configuration du serveur proxy sont corrects](#)".

Échec du package AutoSupport hebdomadaire

Si un colis hebdomadaire AutoSupport échoue à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut « Most Recent Result » sur « Retrying ».
2. Tente de renvoyer le colis AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échecs d'envoi, met à jour l'attribut « Résultat le plus récent » sur Échec.
4. Tente d'envoyer à nouveau un colis AutoSupport à l'heure prévue suivante.
5. Maintient le calendrier régulier AutoSupport si l'envoi du package échoue en raison de l'indisponibilité du service NMS, et si un package est envoyé avant que sept jours ne se soient écoulés.
6. Lorsque le service NMS sera de nouveau disponible, envoie immédiatement un package AutoSupport si aucun package n'a été envoyé depuis sept jours ou plus.

Échec du paquet AutoSupport déclenché par l'utilisateur ou par un événement

Si l'envoi d'un paquet AutoSupport déclenché par l'utilisateur ou par un événement échoue, le système StorageGRID prend les mesures suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir les paramètres de configuration de messagerie corrects, l'erreur suivante s'affiche :
`AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. N'essaie pas de renvoyer le package.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si le protocole SMTP est sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution (**Support > Alarms (legacy) > Legacy Email Setup**). Le message d'erreur suivant peut s'afficher sur la page AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Découvrez comment ["configurer les paramètres du serveur de messagerie"](#).

Corriger une défaillance de package AutoSupport

En cas d'échec et si le protocole SMTP est sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution. Le message d'erreur suivant peut s'afficher sur la page AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyez des packages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer les packages AutoSupport E-Series SANtricity System Manager au support technique via un nœud d'administration StorageGRID plutôt que via le port de gestion de l'appliance de stockage.

Consultez ["Matériel E-Series AutoSupport"](#) pour plus d'informations sur l'utilisation de AutoSupport avec les appliances E-Series.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès administrateur ou Root pour un périphérique de stockage"](#).
- Vous avez configuré SANtricity AutoSupport :
 - Pour les appareils SG6000 et SG5700, ["configurer AutoSupport dans SANtricity System Manager"](#)



Vous devez disposer du firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

À propos de cette tâche

Les packages AutoSupport de la série E contiennent des détails sur le matériel de stockage et sont plus spécifiques que les autres packages AutoSupport envoyés par le système StorageGRID.

Vous pouvez configurer une adresse de serveur proxy spéciale dans SANtricity System Manager pour transmettre des paquets AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les paquets AutoSupport transmis de cette manière sont envoyés par le ["Nœud d'administration de l'expéditeur préféré"](#) et utilisent tous les ["paramètres proxy d'administration"](#) qui ont été configurés dans Grid Manager.

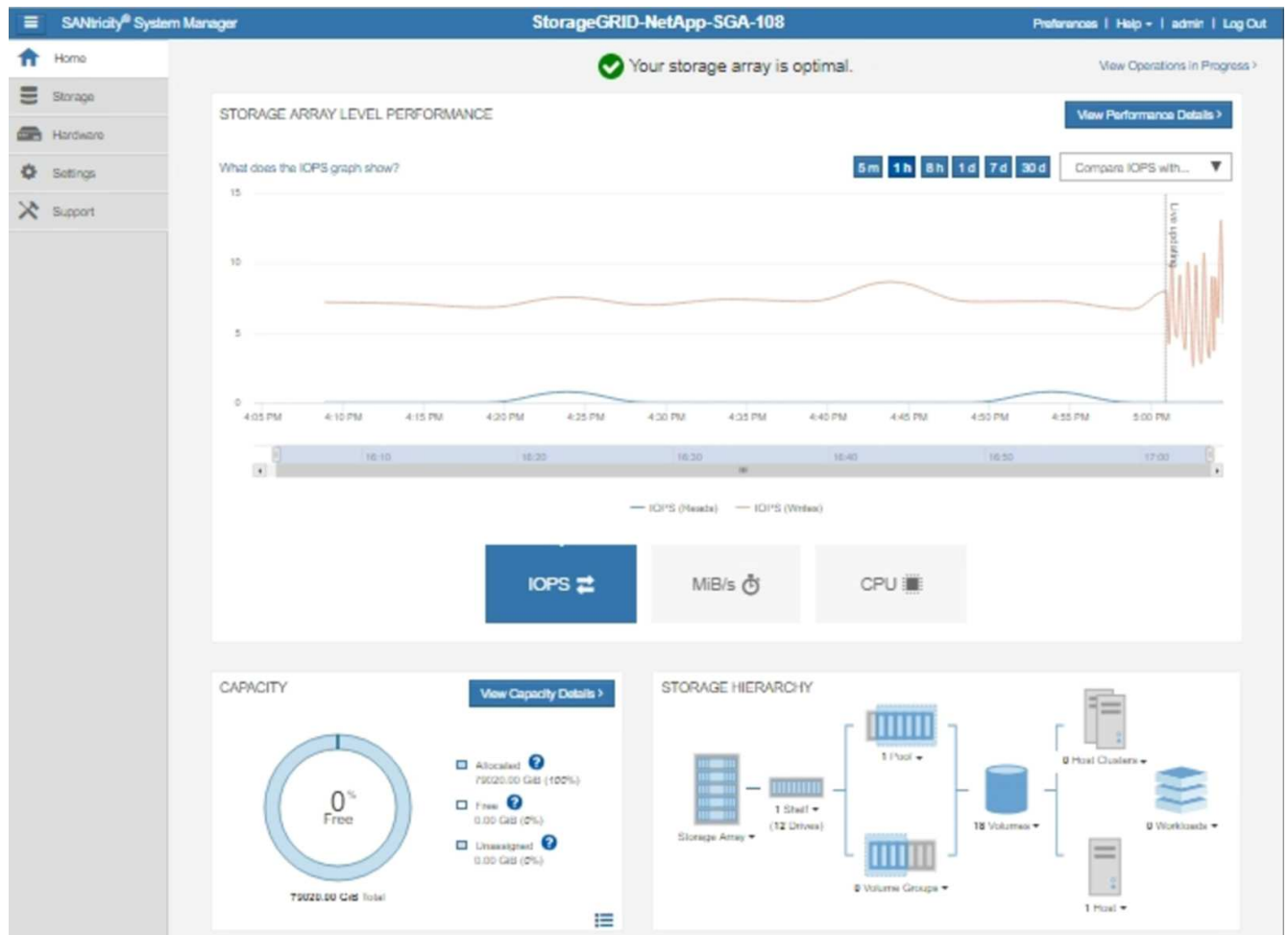


Cette procédure concerne uniquement la configuration d'un serveur proxy StorageGRID pour les packages E-Series AutoSupport. Pour plus de détails sur la configuration E-Series AutoSupport, consultez le ["NetApp Documentation E-Series et SANtricity"](#).

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Nœuds**.
2. Dans la liste des nœuds à gauche, sélectionnez le nœud de l'appliance de stockage que vous souhaitez configurer.
3. Sélectionnez **SANtricity System Manager**.

La page d'accueil de SANtricity System Manager s'affiche.



4. Sélectionnez **Support** > **Support center** > **AutoSupport**.

La page des opérations AutoSupport s'affiche.

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)
AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)
Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)
AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)
Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)
The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)
Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Sélectionnez **Configurer AutoSupport Delivery Method**.

La page Configurer la méthode de livraison AutoSupport s'affiche.

6. Sélectionnez **HTTPS** comme méthode de livraison.



Le certificat qui active le protocole HTTPS est préinstallé.

7. Sélectionnez **via Proxy server**.

8. Saisissez `tunnel-host` pour l'adresse de l'hôte.

`tunnel-host` est l'adresse spéciale à utiliser avec un nœud d'administration pour envoyer des packages AutoSupport E-Series.

9. Saisissez `10225` pour le **numéro de port**.

`10225` correspond au numéro de port sur le serveur proxy StorageGRID qui reçoit les paquets AutoSupport du contrôleur E-Series dans l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport.

Si la configuration est correcte, un message apparaît dans une bannière verte : « Votre AutoSupport configuration a été vérifiée. »

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez vos paramètres DNS et réseau StorageGRID, assurez-vous que "[Nœud d'administration de l'expéditeur préféré](#)" peut se connecter au site de support NetApp, puis réessayez le test.

11. Sélectionnez **Enregistrer**.

La configuration est enregistrée et un message de confirmation apparaît : « AutoSupport delivery method a été configuré. »

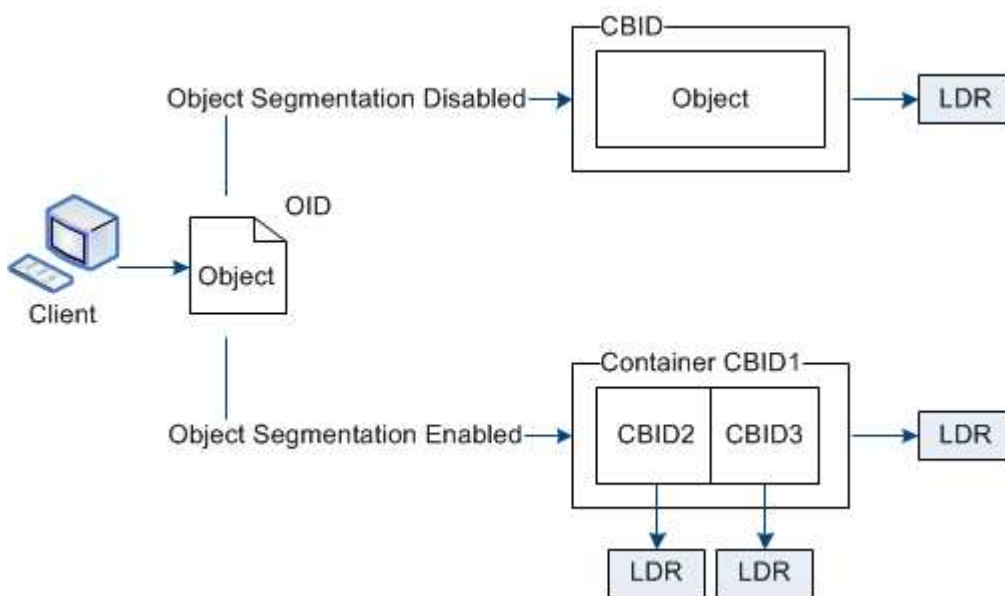
Gérer les nœuds de stockage

Utilisez les options de stockage

Découvrez la segmentation des objets dans StorageGRID

La segmentation d'objets consiste à diviser un objet en une collection d'objets plus petits et de taille fixe afin d'optimiser le stockage et l'utilisation des ressources pour les objets volumineux. Le chargement multipartite S3 crée également des objets segmentés, chaque partie étant représentée par un objet.

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 comme contenu.



Lors de la récupération d'un conteneur de segment, le service LDR assemble l'objet d'origine à partir de ses segments et renvoie l'objet au client.

Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Le conteneur et les segments peuvent être stockés sur n'importe quel nœud de stockage du pool de stockage spécifié dans la règle ILM.

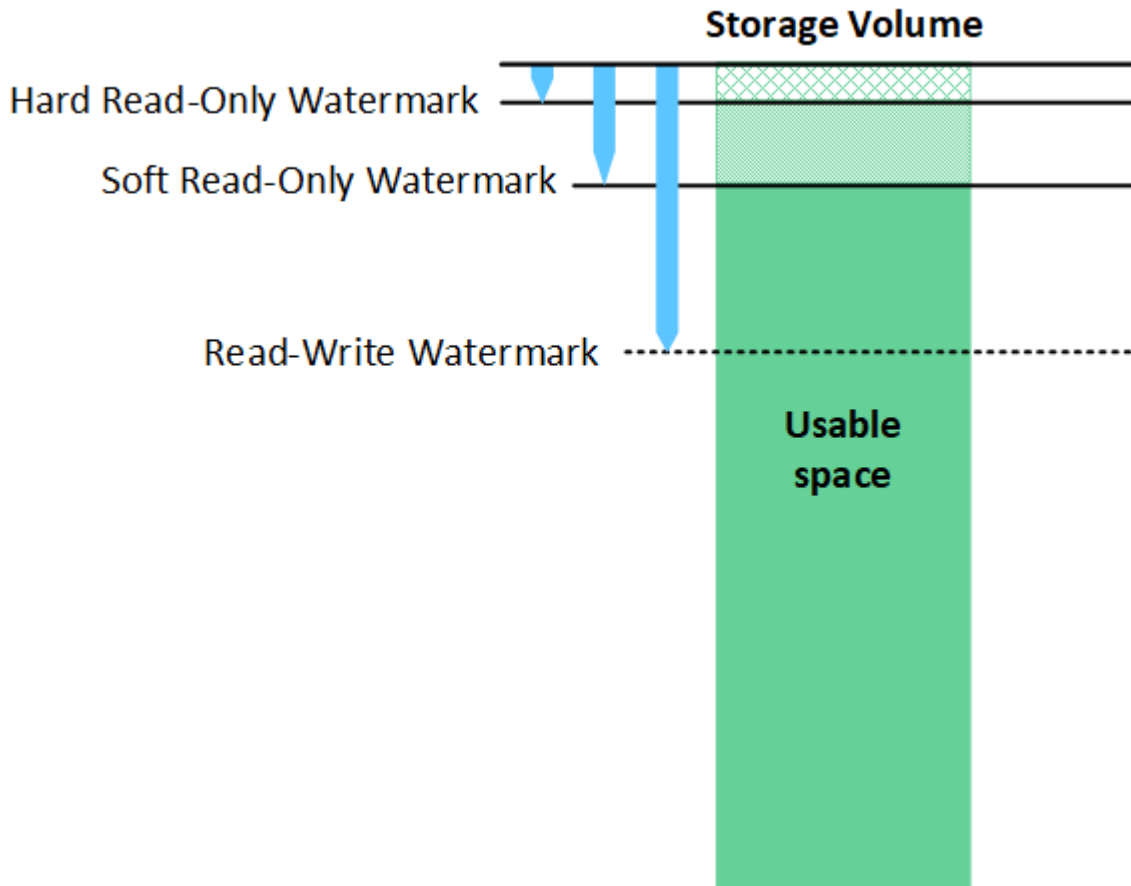
Chaque segment est traité indépendamment par le système StorageGRID et contribue au décompte d'attributs tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID

est divisé en deux segments, la valeur des objets gérés augmente de trois une fois l'ingestion terminée, comme suit :

segment container + segment 1 + segment 2 = three stored objects

Découvrez les seuils de volume de stockage dans StorageGRID

StorageGRID utilise trois marques de volume de stockage pour garantir que les nœuds de stockage passent en toute sécurité en état de lecture seule avant qu'ils n'atteignent un niveau d'espace critique et pour permettre aux nœuds de stockage qui ont été transférés en état de lecture seule de redevenir en lecture-écriture.



Les filigranes de volume de stockage s'appliquent uniquement à l'espace utilisé pour les données d'objets répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées des objets sur le volume 0, accédez à "[Gérer le stockage des métadonnées des objets](#)".

Qu'est-ce que le filigrane souple en lecture seule ?

Le **filigrane de lecture seule logicielle du volume de stockage** est le premier filigrane indiquant que l'espace utilisable d'un nœud de stockage pour les données d'objet est en train de se remplir.

Si l'espace libre de chaque volume d'un nœud de stockage est inférieur au seuil de lecture seule de ce volume, le nœud de stockage passe en *mode lecture seule*. Le mode lecture seule signifie que le nœud de stockage annonce des services de lecture seule au reste du système StorageGRID, mais traite toutes les requêtes d'écriture en attente.

Par exemple, supposons que chaque volume d'un Storage Node possède un seuil de lecture seule souple de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le Storage Node passe en mode lecture seule souple.

Qu'est-ce que le seuil en lecture seule strict ?

Le **filigrane de lecture seule du volume de stockage** est le prochain filigrane indiquant que l'espace utilisable d'un nœud pour les données d'objet est en train de se remplir.

Si l'espace libre sur un volume est inférieur au seuil strict de lecture seule de ce volume, les écritures sur ce volume échoueront. Cependant, les écritures sur d'autres volumes peuvent se poursuivre jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leur seuil strict de lecture seule.

Par exemple, supposons que chaque volume d'un Storage Node possède une limite de lecture seule de 5 Go. Dès que l'espace libre de chaque volume descend en dessous de 5 Go, le Storage Node n'accepte plus aucune requête d'écriture.

Le filigrane en lecture seule physique est toujours inférieur au filigrane en lecture seule logicielle.

Qu'est-ce qu'un watermark de lecture-écriture ?

Le **filigrane de lecture-écriture du volume de stockage** s'applique uniquement aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine à quel moment le nœud peut repasser en mode lecture-écriture. Lorsque l'espace libre sur l'un des volumes de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud repasse automatiquement à l'état de lecture-écriture.

Par exemple, supposons que le nœud de stockage soit passé en mode lecture seule. Supposons également que chaque volume ait une limite de lecture/écriture de 30 Go. Dès que l'espace libre d'un volume atteint 30 Go, le nœud repasse en mode lecture/écriture.

Le filigrane de lecture-écriture est toujours plus grand que le filigrane de lecture seule souple et que le filigrane de lecture seule rigide.

Afficher les filigranes de volume de stockage

Vous pouvez consulter les paramètres actuels du filigrane et les valeurs optimisées par le système. Si les filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez ajuster les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version supérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

Afficher les paramètres de filigrane actuels

Vous pouvez consulter les paramètres actuels de filigrane de stockage dans le Grid Manager.

Étapes

1. Sélectionnez **Support > Other > Storage watermarks**.
2. Sur la page des filigranes de stockage, regardez la case à cocher Utiliser les valeurs optimisées.
 - Si la case est cochée, les trois filigranes sont optimisés pour chaque volume de stockage sur chaque

nœud de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

Il s'agit du paramétrage par défaut et recommandé. Ne modifiez pas ces valeurs. Vous pouvez éventuellement [Afficher les seuils de stockage optimisés](#).

- Si la case « Utiliser les valeurs optimisées » n'est pas cochée, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Utilisez les instructions pour "[Dépannage des alertes de remplacement du seuil bas en lecture seule](#)" déterminer si vous pouvez ou devez ajuster les paramètres.

Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez saisir des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux métriques Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane de lecture seule logicielle du volume de stockage. Vous pouvez consulter les valeurs minimales et maximales optimisées pour chaque nœud de stockage dans votre grid.

1. Sélectionnez **Support > Tools > Metrics**.
2. Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
3. Pour afficher le filigrane minimal recommandé en lecture seule, saisissez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne indique la valeur minimale optimisée du seuil de lecture seule souple pour tous les volumes de stockage sur chaque Storage Node. Si cette valeur est supérieure au paramètre personnalisé du seuil de lecture seule souple du volume de stockage, l'alerte **Low read-only watermark override** est déclenchée pour le Storage Node.

4. Pour afficher la valeur maximale recommandée du filigrane souple en lecture seule, saisissez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne indique la valeur optimisée maximale du filigrane de lecture seule souple pour tous les volumes de stockage sur chaque Storage Node.

Gérez le stockage des métadonnées des objets dans StorageGRID

La capacité de métadonnées des objets d'un système StorageGRID contrôle le nombre maximal d'objets pouvant être stockés sur ce système. Pour garantir que votre système StorageGRID dispose d'un espace suffisant pour stocker de nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées des objets.

Que sont les métadonnées d'un objet ?

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

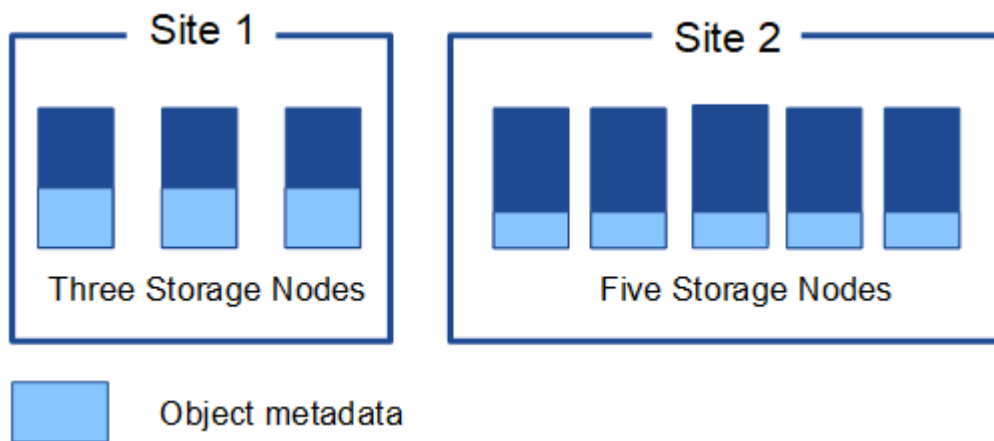
Pour un objet dans StorageGRID, les métadonnées de l'objet comprennent les types d'informations suivants :

- Métadonnées système, y compris un identifiant unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3, le nom ou l'identifiant 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 clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur d'étiquette d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objets dans un Cloud Storage Pool, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multipart, identifiants de segment et tailles de données.

Comment les métadonnées des objets sont-elles stockées ?

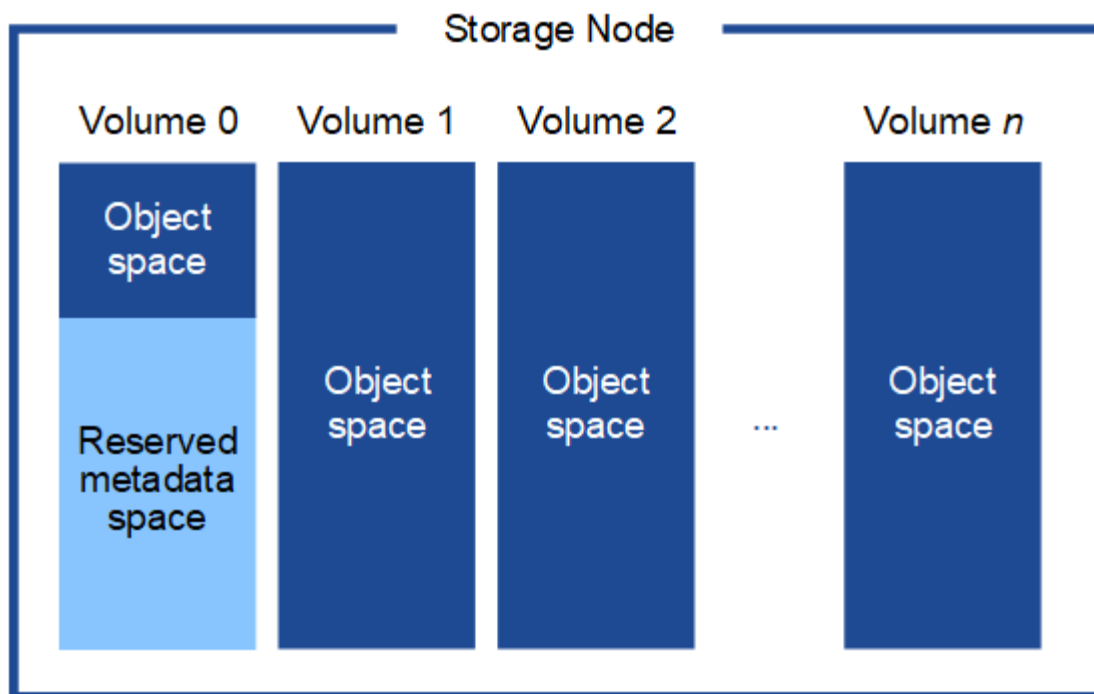
StorageGRID gère les métadonnées des objets dans une base de données Cassandra, qui est stockée indépendamment des données des objets. Afin d'assurer la redondance et de protéger les métadonnées des objets contre toute perte, StorageGRID conserve trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage de deux sites. Chaque site possède la même quantité de métadonnées d'objets, et les métadonnées de chaque site sont subdivisées entre tous les nœuds de stockage de ce site.



Où sont stockées les métadonnées des objets ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve de l'espace pour les métadonnées des objets sur le volume de stockage 0 de chaque nœud de stockage. Il utilise cet espace réservé pour stocker les métadonnées des objets et effectuer des opérations essentielles sur la base de données. Tout espace restant sur le volume de stockage 0 ainsi que sur tous les autres volumes de stockage du nœud de stockage est utilisé exclusivement pour les données des objets (copies répliquées et fragments à codage d'effacement).

La quantité d'espace réservée aux métadonnées des objets sur un nœud de stockage particulier dépend de plusieurs facteurs, qui sont décrits ci-dessous.

Paramètre d'espace réservé aux métadonnées

L'*espace réservé aux métadonnées* est un paramètre à l'échelle du système qui représente la quantité d'espace qui sera réservée aux métadonnées sur le volume 0 de chaque Storage Node. Comme le montre le tableau, la valeur par défaut de ce paramètre est basée sur :

- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- La quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut
11,5 à 12,0	128 Go ou plus sur chaque nœud de stockage de la grille	8 To (8 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage du grid	3 To (3 000 Go)
11,1 à 11,4	128 Go ou plus sur chaque nœud de stockage sur un même site	4 To (4 000 Go)

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut
	Moins de 128 Go sur tout nœud de stockage à chaque site	3 To (3 000 Go)
11.0 ou version antérieure	N'importe quel montant	2 To (2 000 Go)

Afficher le paramètre d'espace réservé pour les métadonnées

Suivez ces étapes pour afficher le paramètre d'espace réservé aux métadonnées de votre système StorageGRID.

Étapes

1. Sélectionnez **Configuration > Système > Paramètres de stockage**.
2. Sur la page des paramètres de stockage, développez la section **Espace réservé aux métadonnées**.

Pour StorageGRID 11.8 ou supérieur, la valeur de l'espace réservé aux métadonnées doit être d'au moins 100 Go et d'au plus 1 Po.

La configuration par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure dans laquelle chaque nœud de stockage dispose de 128 Go ou plus de RAM est de 8 000 Go (8 To).

Espace réellement réservé aux métadonnées

Contrairement au paramètre d'espace réservé aux métadonnées à l'échelle du système, l'espace réellement réservé aux métadonnées des objets est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réellement réservé aux métadonnées dépend de la taille du volume 0 de ce nœud et du paramètre d'espace réservé aux métadonnées à l'échelle du système.

Taille du volume 0 pour le nœud	Espace réellement réservé aux métadonnées
Moins de 500 Go (utilisation hors production)	10% du volume 0
500 Go ou plus + ou + Nœuds de stockage uniquement pour les métadonnées	La plus petite de ces valeurs : • Volume 0 • Paramètre d'espace réservé aux métadonnées Remarque : Un seul rangedb est requis pour les nœuds de stockage uniquement de métadonnées.

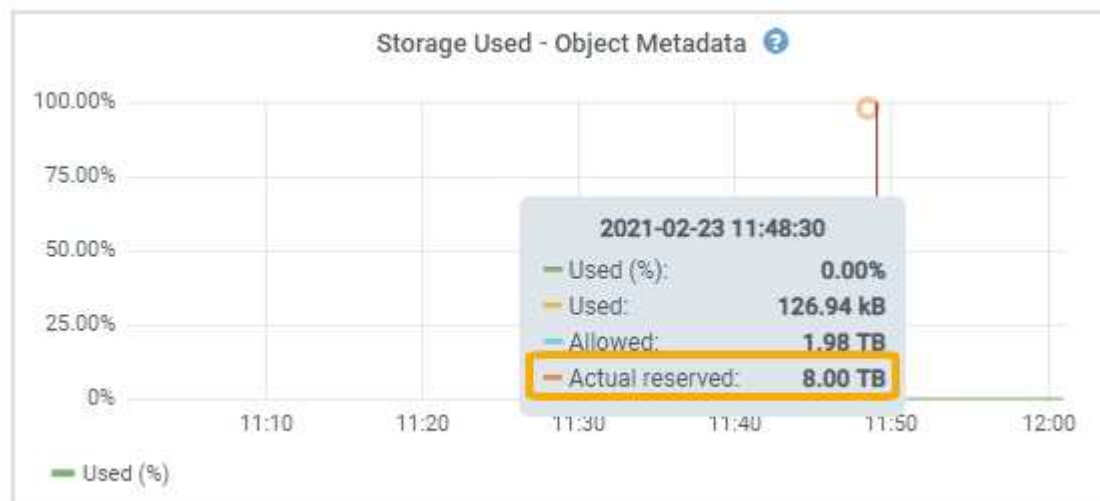
Afficher l'espace réellement réservé aux métadonnées

Suivez ces étapes pour afficher l'espace réellement réservé aux métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans le Grid Manager, sélectionnez **Nœuds > Storage Node**.

2. Sélectionnez l'onglet **Storage**.
3. Placez votre curseur sur le graphique « Storage Used - Object Metadata » et repérez la valeur **Actual reserved**.



Sur la capture d'écran, la valeur **Réservé réel** est de 8 To. Cette capture d'écran concerne un grand Storage Node dans une nouvelle installation StorageGRID 11.6. Parce que le paramètre d'espace réservé aux métadonnées à l'échelle du système est inférieur au volume 0 pour ce Storage Node, l'espace réellement réservé pour ce nœud est égal au paramètre d'espace réservé aux métadonnées.

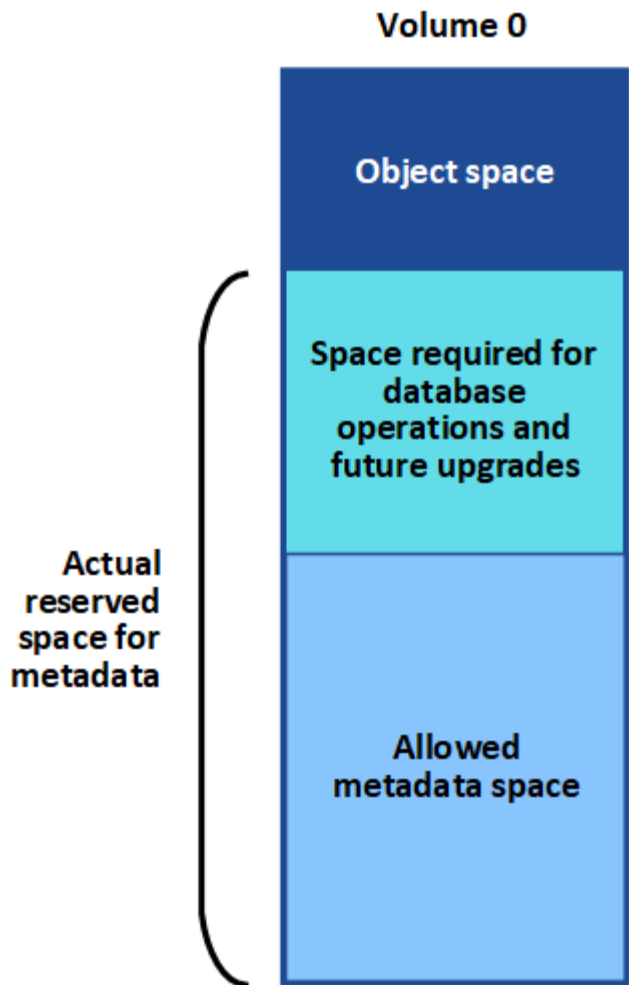
Exemple d'espace de métadonnées réellement réservé

Supposons que vous installiez un nouveau système StorageGRID en utilisant la version 11.7 ou ultérieure. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réellement réservé aux métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)

Espace autorisé pour les métadonnées

L'espace réservé aux métadonnées de chaque nœud de stockage est subdivisé en l'espace disponible pour les métadonnées des objets (l'espace autorisé pour les métadonnées) et l'espace requis pour les opérations essentielles de la base de données (telles que la compaction et la réparation) ainsi que pour les futures mises à niveau matérielles et logicielles. L'espace autorisé pour les métadonnées 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 réellement réservé aux métadonnées.

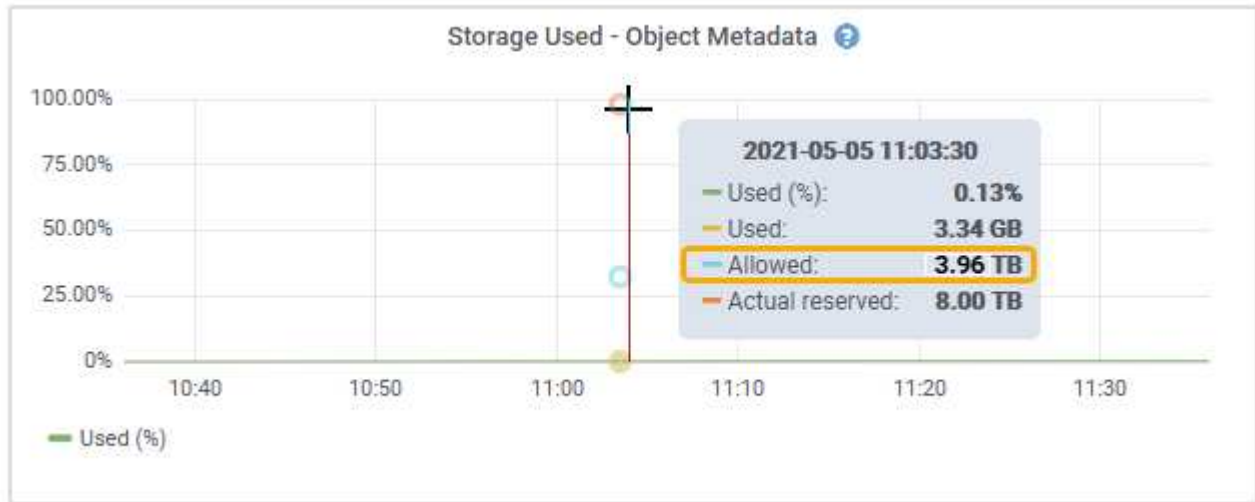
	Quantité de mémoire sur le nœud de stockage		
	< 128 Go	≥ 128 Go	Espace réellement réservé aux métadonnées
≤ 4 To	60 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,32 To	60 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,98 To	4 To

Afficher l'espace de métadonnées autorisé

Suivez ces étapes pour afficher l'espace de métadonnées autorisé pour un Storage Node.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Nœuds**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **Storage**.
4. Placez votre curseur sur le graphique « Storage used - object metadata » et repérez la valeur **Allowed**.



Sur la capture d'écran, la valeur **Autorisée** est de 3,96 To, ce qui correspond à la valeur maximale pour un Storage Node dont l'espace réellement réservé aux métadonnées est supérieur à 4 To.

La valeur **Allowed** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installiez un système StorageGRID en version 11.6. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.6 ou version ultérieure lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réellement réservé aux métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, basé sur le calcul indiqué dans le [tableau de l'espace autorisé pour les métadonnées](#) : (Espace réellement réservé pour les métadonnées – 1 To) × 60 %, jusqu'à un maximum de 3,96 To.

Comment les nœuds de stockage de différentes tailles affectent la capacité des objets

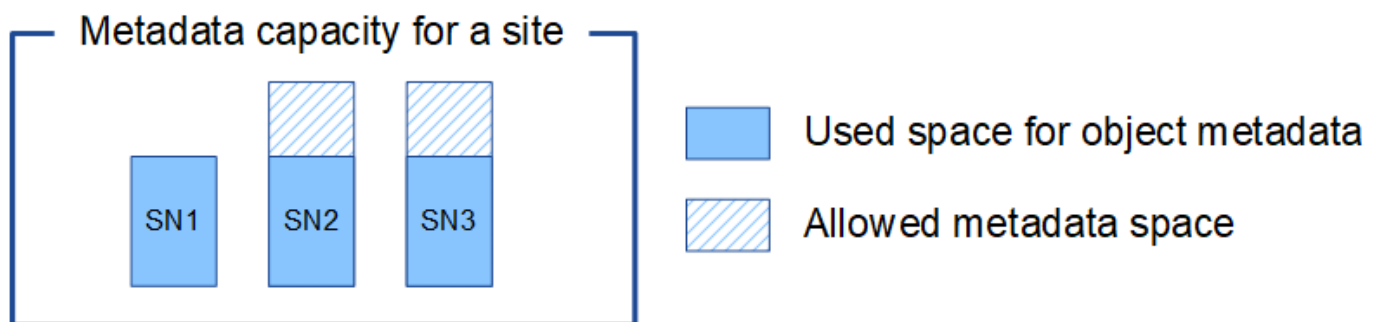
Comme indiqué précédemment, StorageGRID répartit uniformément les métadonnées des objets entre les nœuds de stockage de chaque site. Pour cette raison, si un site contient des nœuds de stockage de tailles différentes, le plus petit nœud du site détermine la capacité de métadonnées du site.

Considérez l'exemple suivant :

- Vous disposez d'une grille à site unique contenant trois nœuds de stockage de tailles différentes.
- Le paramètre **Espace réservé aux métadonnées** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace de métadonnées réellement réservé et l'espace de métadonnées autorisé.

Nœud de stockage	Taille du volume 0	Espace de métadonnées réellement réservé	Espace autorisé pour les métadonnées
SN1	2,2 To	2,2 To	1,32 To
SN2	5 To	4 To	1,98 To
SN3	6 To	4 To	1,98 To

Étant donné que les métadonnées des objets sont réparties uniformément entre les nœuds de stockage d'un site, 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, étant donné que StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale de métadonnées d'un système StorageGRID est déterminée par la capacité de métadonnées d'objet du plus petit site.

Et comme la capacité des métadonnées des objets contrôle le nombre maximal d'objets, lorsqu'un nœud n'a plus de capacité de métadonnées, la grille est effectivement pleine.

Informations connexes

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, consultez les instructions pour ["Surveillance StorageGRID"](#).
- Pour augmenter la capacité de métadonnées d'objets de votre système, ["étendre une grille"](#) en ajoutant de nouveaux nœuds de stockage.

Augmentez le paramètre Metadata Reserved Space dans StorageGRID

Vous pouvez peut-être augmenter le paramètre système « Espace réservé aux métadonnées » si vos nœuds de stockage répondent à des exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous aurez besoin

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès racine ou autorisation de configuration de la grille Other"](#).

À propos de cette tâche

Vous pourrez peut-être augmenter manuellement le paramètre d'espace réservé aux métadonnées à l'échelle du système jusqu'à 8 To.

Vous ne pouvez augmenter la valeur du paramètre « Espace réservé aux métadonnées » à l'échelle du système que si les deux conditions suivantes sont vraies :

- Les nœuds de stockage sur n'importe quel site de votre système disposent chacun de 128 Go de RAM ou plus.
- Chaque nœud de stockage sur n'importe quel site de votre système dispose d'un espace disponible suffisant sur le volume de stockage 0.

Notez que si vous augmentez cette valeur, vous réduirez simultanément l'espace disponible pour le stockage d'objets sur le volume de stockage 0 de tous les Storage Nodes. Pour cette raison, vous pourriez préférer définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction de vos besoins estimés en métadonnées d'objets.



En général, il est préférable d'utiliser une valeur élevée plutôt qu'une valeur faible. Si le paramètre « Espace réservé aux métadonnées » est trop important, vous pouvez le réduire ultérieurement. En revanche, si vous augmentez cette valeur par la suite, le système pourrait devoir déplacer des données d'objet pour libérer de l'espace.

Pour une explication détaillée de la manière dont le paramètre Espace réservé aux métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, voir ["Gérer le stockage des métadonnées des objets"](#).

Étapes

1. Déterminez le paramètre actuel d'espace réservé aux métadonnées.
 - a. Sélectionnez **Configuration > Système > Paramètres de stockage**.
 - b. Notez la valeur de **Metadata Reserved Space**.
2. Assurez-vous de disposer de suffisamment d'espace disponible sur le volume de stockage 0 de chaque Storage Node pour augmenter cette valeur.
 - a. Sélectionnez **Nœuds**.
 - b. Sélectionnez le premier nœud de stockage dans la grille.
 - c. Sélectionnez l'onglet **Storage**.
 - d. Dans la section **Volumes**, repérez l'entrée **/var/local/rangedb/0**.
 - e. Confirmez que la valeur disponible est égale ou supérieure à la différence entre la nouvelle valeur que vous souhaitez utiliser et la valeur actuelle de l'espace réservé aux métadonnées.

Par exemple, si le paramètre Espace réservé aux métadonnées est actuellement de 4 To et que vous souhaitez l'augmenter à 6 To, la valeur Disponible doit être de 2 To ou plus.

- f. Répétez ces étapes pour tous les nœuds de stockage.
 - Si un ou plusieurs nœuds de stockage ne disposent pas d'un espace suffisant, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette

procédure.

- Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.

3. Assurez-vous de disposer d'au moins 128 Go de RAM sur chaque nœud de stockage.

- Sélectionnez **Nœuds**.
- Sélectionnez le premier nœud de stockage dans la grille.
- Sélectionnez l'onglet **Matériel**.
- Placez votre curseur sur le graphique d'utilisation de la mémoire. Assurez-vous que **Total Memory** est d'au moins 128 Go.
- Répétez ces étapes pour tous les nœuds de stockage.
 - Si un ou plusieurs nœuds de stockage ne disposent pas d'une mémoire totale suffisante, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.
 - Si chaque nœud de stockage possède au moins 128 Go de mémoire totale, passez à l'étape suivante.

4. Mettez à jour le paramètre Espace réservé aux métadonnées.

- Sélectionnez **Configuration > Système > Paramètres de stockage**.
- Sélectionnez **Espace réservé aux métadonnées**.
- Saisissez la nouvelle valeur.

Par exemple, pour saisir 8 To, qui est la valeur maximale prise en charge, saisissez **8000000000000** (8 suivi de 12 zéros)

- Sélectionnez **Enregistrer**.

Compresser les objets stockés dans StorageGRID

Vous pouvez activer la compression des objets pour réduire la taille des objets stockés dans StorageGRID, afin que les objets consomment moins de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

À propos de cette tâche

Par défaut, la compression des objets est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement en utilisant une compression sans perte.



Si vous modifiez ce paramètre, il faudra environ une minute pour que le nouveau paramètre soit appliqué. La valeur configurée est mise en cache pour optimiser les performances et la mise à l'échelle.

Avant d'activer la compression d'objets, veuillez prendre en compte les points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés** sauf si vous savez que les données stockées sont compressibles.

- Les applications qui enregistrent des objets dans StorageGRID peuvent les compresser avant l'enregistrement. Si une application cliente a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille de l'objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si l'option **Compresser les objets stockés** est sélectionnée, les applications clientes S3 doivent éviter d'effectuer des opérations GetObject qui spécifient le retour d'une plage d'octets. Ces opérations de « lecture par plage » sont inefficaces car StorageGRID doit effectivement décompresser les objets pour accéder aux octets demandés. Les opérations GetObject qui demandent une petite plage d'octets à partir d'un objet très volumineux sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les requêtes client peuvent expirer.



Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures par plage, augmentez le délai d'expiration de lecture pour l'application.

Étapes

1. Sélectionnez **Configuration > Système > Paramètres de stockage > Compression des objets**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer les nœuds de stockage complets dans StorageGRID

Lorsque les nœuds de stockage atteignent leur capacité maximale, vous devez étendre le système StorageGRID en ajoutant du stockage supplémentaire. Trois options s'offrent à vous : ajouter des volumes de stockage, ajouter des étagères d'expansion de stockage et ajouter des nœuds de stockage.

Ajouter des volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plateforme. Si un nœud de stockage contient moins que le nombre maximal de volumes de stockage, vous pouvez ajouter des volumes pour augmenter sa capacité. Consultez les instructions pour ["extension d'un système StorageGRID"](#).

Ajouter des étagères d'extension de stockage

Certains nœuds de stockage StorageGRID, tels que le SG6060 ou le SG6160, peuvent prendre en charge des étagères de stockage supplémentaires. Si vous disposez d'appliances StorageGRID avec des capacités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des étagères de stockage pour augmenter la capacité. Consultez les instructions pour ["extension d'un système StorageGRID"](#).

Ajouter des nœuds de stockage

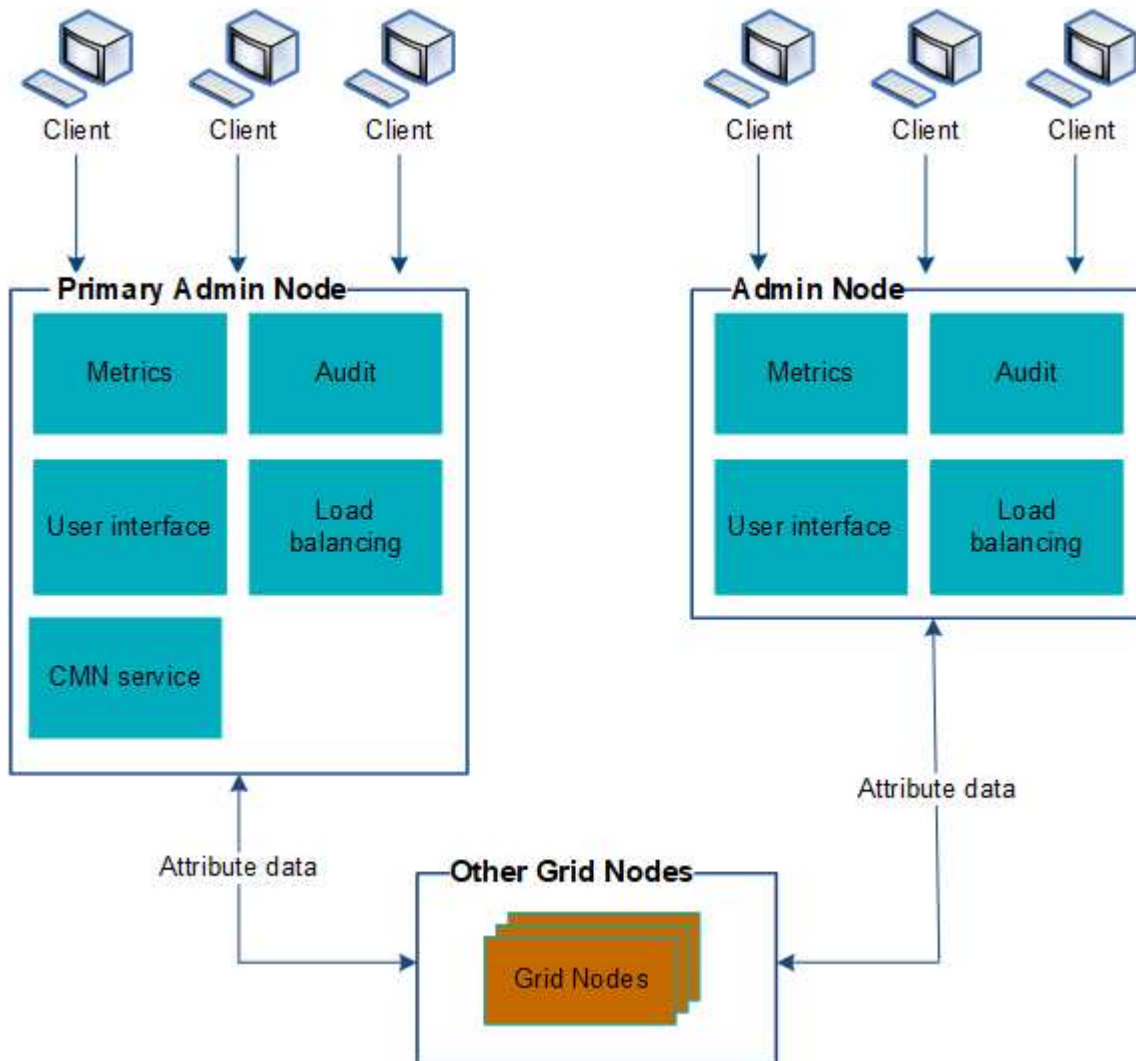
Vous pouvez augmenter la capacité de stockage en ajoutant des nœuds de stockage. Une attention particulière doit être portée aux règles ILM actuellement actives et aux exigences de capacité lors de l'ajout de stockage. Consultez les instructions pour ["extension d'un système StorageGRID"](#).

Gérer les nœuds d'administration

Utilisez plusieurs nœuds d'administration dans StorageGRID

Un système StorageGRID peut inclure plusieurs nœuds d'administration afin de vous permettre de surveiller et de configurer en continu votre système StorageGRID, même si un nœud d'administration tombe en panne.

Si un nœud d'administration devient indisponible, le traitement des attributs se poursuit, les alertes sont toujours déclenchées et les notifications par e-mail ainsi que les packages AutoSupport sont toujours envoyés. Cependant, la présence de plusieurs nœuds d'administration n'offre une protection contre les pannes que pour les notifications et les packages AutoSupport.



Deux options permettent de continuer à visualiser et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à n'importe quel autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration à haute disponibilité, les clients web peuvent continuer à accéder au Grid Manager ou au Tenant Manager en utilisant l'adresse IP virtuelle du groupe HA. Voir "[Gérer les groupes à haute disponibilité](#)".



Lors de l'utilisation d'un groupe HA, l'accès est interrompu en cas de défaillance du nœud d'administration actif. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA a basculé vers un autre nœud d'administration du groupe.

Certaines opérations de maintenance ne peuvent être effectuées qu'à l'aide du nœud d'administration principal. Si le nœud d'administration principal tombe en panne, il doit être restauré avant que le système StorageGRID ne soit de nouveau pleinement opérationnel.

Identifiez le nœud d'administration principal dans StorageGRID

Le nœud d'administration principal offre plus de fonctionnalité que les nœuds d'administration non principaux. Par exemple, certaines procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

Pour plus d'informations sur les nœuds d'administration, voir ["Qu'est-ce qu'un nœud d'administration"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **Nœuds**.
2. Saisissez **primary** dans le champ de recherche.

Dans les résultats de la recherche, identifiez le nœud dont la colonne Type affiche « Primary Admin Node ». Un seul Primary Admin Node doit être affiché.

Gérez les objets avec ILM

Gérez les objets avec ILM dans StorageGRID

`${post_edited_translations.segment}`

À propos de ces instructions

La conception et la mise en œuvre des règles et politiques ILM nécessitent une planification rigoureuse. Vous devez comprendre 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 souhaitez que les différents types d'objets soient copiés, distribués et stockés.

Utilisez ces instructions pour :

- Découvrez l'ILM StorageGRID, notamment ["Comment l'ILM fonctionne tout au long du cycle de vie d'un objet"](#).
- Apprenez à configurer ["pools de stockage"](#), ["Pools de stockage cloud"](#) et ["Règles ILM"](#).
- Découvrez comment ["\\${post_edited_translations.segment}"](#) protéger les données d'objets sur un ou plusieurs sites.
- Découvrez comment ["Gérez les objets avec S3 Object Lock"](#), ce qui permet de garantir que les objets dans des compartiments S3 spécifiques ne sont ni supprimés ni écrasés pendant une période déterminée.

En savoir plus

Pour en savoir plus, consultez ces vidéos :

[Aperçu des règles ILM](#)

[Aperçu des politiques ILM](#)

`${post_edited_translations.segment}`

Fonctionnement de l'ILM tout au long du cycle de vie d'un objet dans StorageGRID

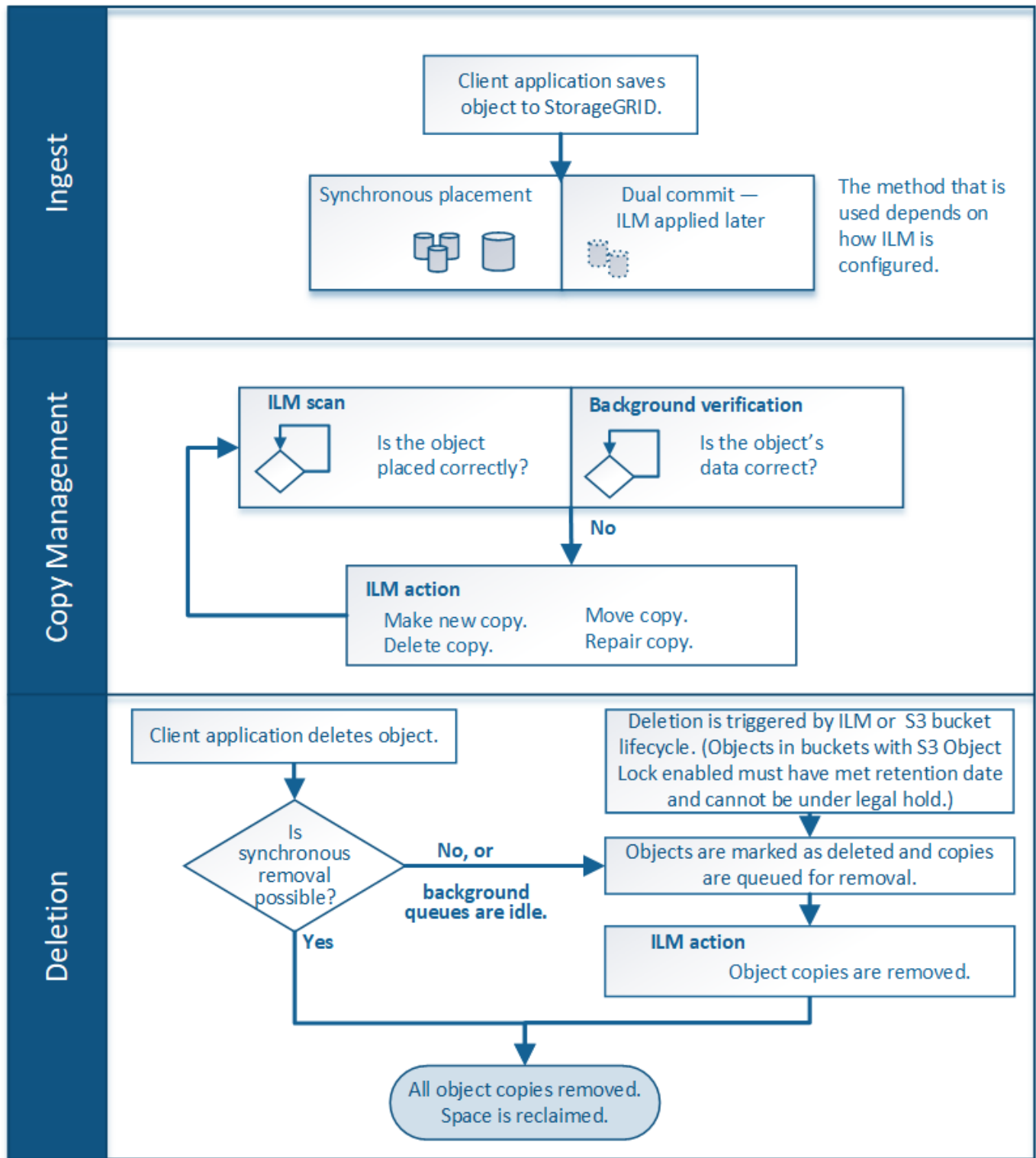
Comprendre comment StorageGRID utilise ILM pour gérer les objets à chaque étape de leur cycle de vie peut vous aider à concevoir une politique plus efficace.

- **Ingestion** : L'ingestion commence lorsqu'une application cliente S3 établit une connexion pour enregistrer un objet dans le système StorageGRID et se termine lorsque StorageGRID renvoie un message « ingestion réussie » au client. Les données de l'objet sont protégées pendant l'ingestion soit par l'application immédiate des instructions ILM (placement synchrone), soit par la création de copies intermédiaires et l'application ultérieure des instructions ILM (double validation), selon la façon dont les exigences ILM ont été spécifiées.
- **Gestion des copies** : Après avoir créé le nombre et le type de copies d'objets spécifiés dans les instructions de placement de l'ILM, StorageGRID gère les emplacements des objets et protège les objets contre la perte de données.
 - **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 des copies d'objets de types, de nombres ou d'emplacements différents sont nécessaires, StorageGRID crée, supprime ou déplace les copies selon les besoins.
 - **Vérification en arrière-plan** : StorageGRID effectue en continu une vérification en arrière-plan afin de contrôler l'intégrité des données des objets. En cas de problème, StorageGRID crée automatiquement une nouvelle copie de l'objet ou un fragment d'objet de remplacement code d'effacement, dans un emplacement conforme aux exigences ILM actuelles. Voir "[Vérifiez l'intégrité de l'objet](#)".
- **Suppression d'objet** : La gestion d'un objet prend fin lorsque toutes ses copies sont supprimées du système StorageGRID. Les objets peuvent être supprimés suite à une demande de suppression d'un client, par ILM ou à la suite de la suppression causée par l'expiration du cycle de vie d'un compartiment S3.



Les objets d'un compartiment pour lequel le verrouillage d'objets S3 est activé ne peuvent pas être supprimés s'ils font l'objet d'une conservation légale ou si une date limite de conservation a été spécifiée mais n'a pas encore été atteinte.

Le diagramme résume le fonctionnement d'ILM tout au long du cycle de vie d'un objet.



`${post_edited_translations.segment}`

Options d'ingestion ILM dans StorageGRID

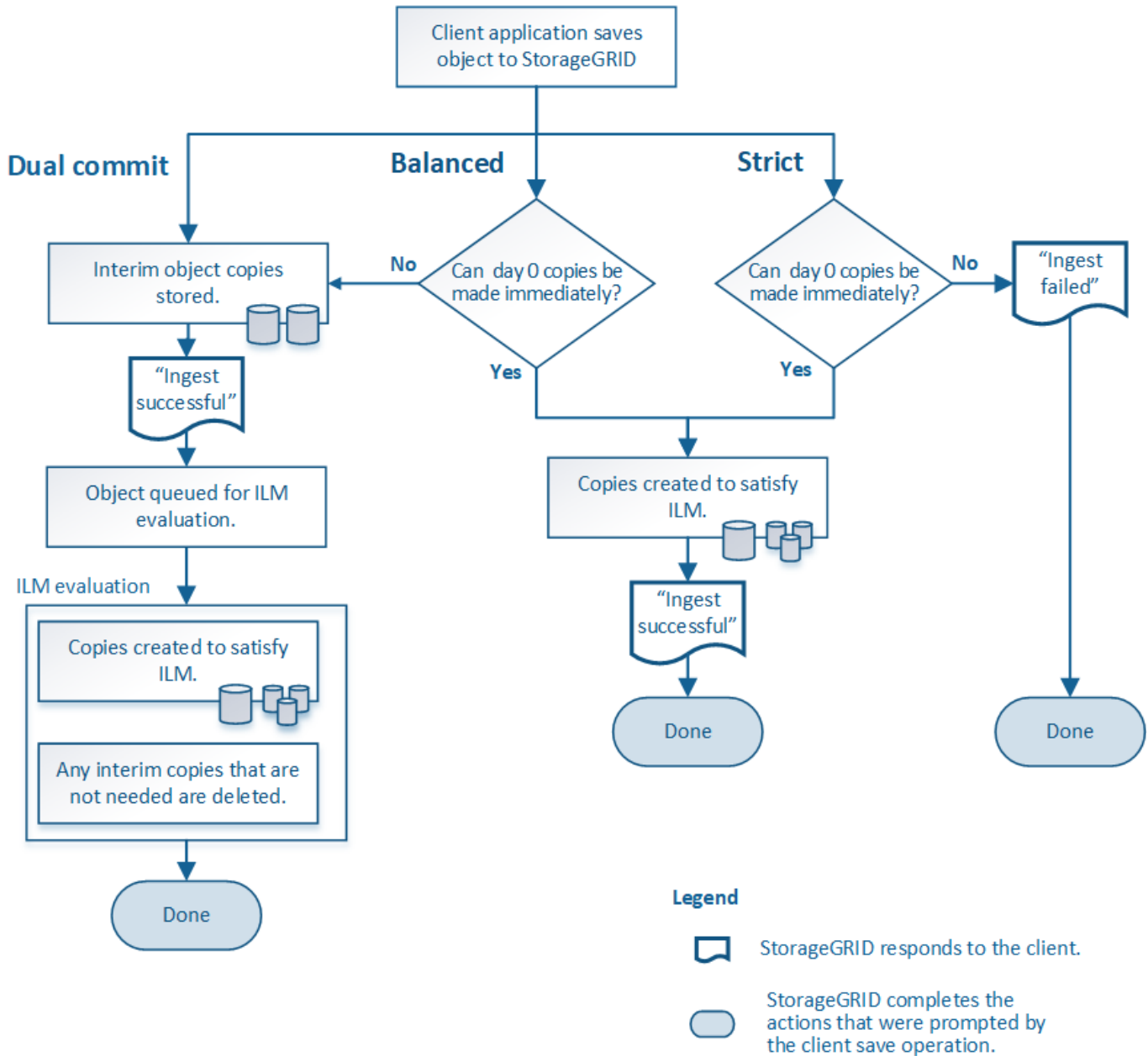
Lorsque vous créez une règle ILM, vous spécifiez l'une des trois options suivantes pour protéger les objets lors de l'ingestion : Dual commit, Strict ou Balanced.

Selon votre choix, StorageGRID effectue des copies intermédiaires et met les objets en file d'attente pour une

évaluation ILM ultérieure, ou il utilise un placement synchrone et effectue immédiatement des copies pour répondre aux exigences ILM.

Organigramme des options d'ingestion

Le diagramme de flux montre ce qui se passe lorsque des objets correspondent à une règle ILM utilisant chacune des trois options d'ingestion.



Double engagement

Lorsque vous sélectionnez l'option Double validation, StorageGRID crée immédiatement des copies intermédiaires de l'objet sur deux nœuds de stockage différents et renvoie un message "ingestion réussie" au client. L'objet est mis en file d'attente pour l'évaluation ILM, et des copies conformes aux instructions de placement de la règle sont créées ultérieurement. Si la politique ILM ne peut pas être traitée immédiatement après la double validation, la protection contre la perte de site peut prendre du temps à être atteinte.

Utilisez l'option de double validation dans l'un ou l'autre de ces cas :

- Vous utilisez des règles ILM multisites et la latence d'ingestion côté client est votre principale préoccupation. Lorsque vous utilisez le double commit, vous devez vous assurer que votre grille peut effectuer le travail supplémentaire de création et de suppression des copies de double commit si elles ne satisfont pas l'ILM. Plus précisément :
 - La charge sur la grille doit être suffisamment faible pour éviter un retard ILM.
 - Le réseau doit disposer de ressources matérielles excédentaires (IOPS, CPU, mémoire, bande passante réseau, etc.).
- Vous utilisez des règles ILM multisites et la connexion WAN entre les sites présente généralement une latence élevée ou une bande passante limitée. Dans ce scénario, l'option Dual commit peut aider à éviter les délais d'attente côté client. Avant de choisir l'option Dual commit, vous devez tester l'application cliente avec des charges de travail réalistes.

Équilibré (par défaut)

Lorsque vous sélectionnez l'option Équilibré, StorageGRID utilise également le placement synchrone lors de l'ingestion et crée immédiatement toutes les copies spécifiées dans les instructions de placement de la règle. Contrairement à l'option Strict, si StorageGRID ne peut pas créer immédiatement toutes les copies, il utilise la double validation à la place. Si la politique ILM utilise des placements sur plusieurs sites et qu'une protection immédiate contre la perte de site ne peut être assurée, l'alerte **ILM placement unachievable** est déclenchée.

Utilisez l'option Équilibrée pour obtenir le meilleur compromis entre protection des données, performances de la grille et taux de réussite de l'ingestion. L'option Équilibrée est l'option par défaut de l'assistant de création de règles ILM.

Strict

Lorsque vous sélectionnez l'option Strict, StorageGRID utilise un placement synchrone lors de l'ingestion et crée immédiatement toutes les copies d'objets spécifiées dans les instructions de placement de la règle. L'ingestion échoue si StorageGRID ne peut pas créer toutes les copies, par exemple si un emplacement de stockage requis est temporairement indisponible. Le client doit réessayer l'opération.

Utilisez l'option Strict si vous avez une obligation opérationnelle ou réglementaire de stocker immédiatement les objets uniquement aux emplacements définis dans la règle ILM. Par exemple, pour satisfaire à une exigence réglementaire, vous pourriez devoir utiliser l'option Strict et un filtre avancé de Location Constraint afin de garantir que les objets ne soient jamais stockés dans certains centres de données.

Voir ["Exemple 5 : Règles et politique ILM pour le comportement d'ingestion strict"](#).

Avantages, inconvénients et limitations des options d'ingestion ILM dans StorageGRID

Comprendre les avantages et les inconvénients de chacune des trois options de protection des données lors de l'ingestion (Balanced, Strict ou Dual commit) peut vous aider à décider laquelle choisir pour une règle ILM.

Pour un aperçu des options d'ingestion, voir ["Options d'ingestion"](#).

Avantages des options équilibrée et stricte

Comparées à la validation double, qui crée des copies intermédiaires lors de l'ingestion, les deux options de placement synchrone peuvent offrir les avantages suivants :

- **Meilleure sécurité des données** : Les données objet sont immédiatement protégées conformément aux instructions de placement de la règle ILM, qui peuvent être configurées pour se prémunir contre un large

éventail de défaillances, y compris la défaillance de plus d'un emplacement de stockage. La double validation ne protège que contre la perte d'une seule copie locale.

- **Fonctionnement plus efficace de la grille** : chaque objet n'est traité qu'une seule fois, lors de son ingestion. Parce que le système StorageGRID n'a pas besoin de suivre ni de supprimer les copies intermédiaires, la charge de traitement est réduite et moins d'espace de base de données est consommé.
- **(Équilibré) Recommandé** : L'option Équilibré offre une efficacité ILM optimale. L'utilisation de l'option Équilibré est recommandée, sauf si un comportement d'ingestion strict est requis ou si la grille remplit tous les critères pour l'utilisation de Dual commit.
- **(Strict) Certitude quant à l'emplacement des objets** : L'option Strict garantit que les objets sont immédiatement stockés conformément aux instructions de placement de la règle ILM.

Inconvénients des options équilibrée et stricte

Comparées à l'option Dual commit, les options Balanced et Strict présentent certains inconvénients :

- **Ingestion côté client plus longue** : La latence d'ingestion côté client peut être plus longue. Lorsque vous utilisez les options Balanced ou Strict, un message « ingestion réussie » n'est pas renvoyé au client tant que tous les fragments à code d'effacement ou les copies répliquées n'ont pas été créés et stockés. Cependant, les données des objets atteindront très probablement leur emplacement final beaucoup plus rapidement.
- **(Strict) Taux d'échec d'ingestion plus élevés** : Avec l'option Strict, l'ingestion échoue si StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle ILM. Vous pouvez constater des taux d'échec d'ingestion élevés si un emplacement de stockage requis est temporairement hors ligne ou si des problèmes réseau entraînent des retards dans la copie des objets entre les sites.
- **(Strict) Le placement des objets lors d'un chargement multipartie S3 peut ne pas être conforme à vos attentes dans certaines circonstances** : Avec Strict, vous vous attendez à ce que les objets soient placés comme décrit par la règle ILM ou que l'ingestion échoue. Cependant, lors d'un chargement multipartie S3, l'ILM est évalué pour chaque partie de l'objet au fur et à mesure de son ingestion, puis pour l'objet dans son ensemble lorsque le chargement multipartie est terminé. Dans les circonstances suivantes, cela peut entraîner des placements différents de ceux auxquels vous vous attendez :
 - **Si les règles ILM changent pendant un chargement multipartie S3** : chaque partie étant placée selon la règle active au moment de son ingestion, certaines parties de l'objet peuvent ne pas respecter les exigences ILM actuelles une fois le chargement multipartie terminé. Dans ces cas, l'ingestion de l'objet n'échoue pas. Au lieu de cela, toute partie mal placée est mise en file d'attente pour une réévaluation ILM et déplacée ultérieurement vers l'emplacement correct.
 - **Lorsque les règles ILM filtrent par taille** : Lors de l'évaluation ILM d'une partie, StorageGRID filtre sur la taille de la partie, et non sur celle de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements ne répondant pas aux exigences ILM de l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés à DC1 tandis que tous les objets plus petits sont stockés à DC2, lors de l'ingestion, chaque partie de 1 Go d'un chargement multipartie en 10 parties est stockée à DC2. Lors de l'évaluation ILM de l'objet, toutes les parties de l'objet sont déplacées vers DC1.
- **(Strict) L'ingestion ne rencontre pas d'échec lorsque les balises ou les métadonnées d'un objet sont mises à jour et que les nouveaux emplacements requis ne peuvent pas être effectués** : Avec Strict, vous vous attendez à ce que les objets soient soit placés comme décrit par la règle ILM, soit que l'ingestion échoue. Cependant, lorsque vous mettez à jour les métadonnées ou les balises d'un objet déjà stocké dans la grille, l'objet n'est pas réingéré. Cela signifie que toute modification de l'emplacement de l'objet déclenchée par la mise à jour n'est pas appliquée immédiatement. Les modifications d'emplacement sont effectuées lorsque l'ILM est réévalué par les processus ILM d'arrière-plan normaux. Si les modifications d'emplacement requises ne peuvent pas être effectuées (par exemple, parce qu'un nouvel emplacement requis est indisponible), l'objet mis à jour conserve son emplacement actuel jusqu'à ce que

les modifications soient possibles.

Limitations du placement des objets avec les options **Balanced** et **Strict**

Les options **Équilibré** ou **Strict** ne peuvent pas être utilisées pour les règles ILM qui comportent l'une de ces instructions de placement :

- Placement dans un Cloud Storage Pool au jour 0.
- Placements dans un Cloud Storage Pool lorsque la règle a une date de création définie par l'utilisateur comme heure de référence.

Ces restrictions existent car StorageGRID ne peut pas effectuer de copies synchrones vers un Cloud Storage Pool, et une date de création définie par l'utilisateur peut correspondre à la date actuelle.

Comment les règles ILM et la cohérence interagissent pour affecter la protection des données

La manière dont les objets sont protégés dépend à la fois de votre règle ILM et de votre choix de cohérence. Ces paramètres peuvent interagir.

Par exemple, le comportement d'ingestion sélectionné pour une règle ILM influe sur l'emplacement initial des copies d'objets, tandis que la cohérence utilisée lors du stockage d'un objet influe sur l'emplacement initial de ses métadonnées. Étant donné que StorageGRID nécessite l'accès aux données et aux métadonnées d'un objet pour répondre aux requêtes client, le choix de niveaux de protection identiques pour la cohérence et le comportement d'ingestion permet une meilleure protection des données et des réponses système plus prévisibles.

Voici un bref résumé des valeurs de cohérence disponibles dans StorageGRID :

- **Tous** : Tous les nœuds reçoivent immédiatement les métadonnées de l'objet ou la requête échouera.
- **Forte-globale** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client sur tous les sites. Lorsque la sémantique de quorum est configurée, les comportements suivants s'appliquent :
 - Permet une tolérance aux pannes de site pour les requêtes client lorsque les grilles comportent trois sites ou plus. Les grilles à deux sites n'ont pas de tolérance aux pannes de site.
 - Les opérations S3 suivantes ne pourront pas aboutir si l'un des sites est hors service :
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si nécessaire, vous pouvez ["Configurer la sémantique de quorum de StorageGRID pour une cohérence globale forte"](#).

- **Strong-site** : les métadonnées des objets sont immédiatement distribuées aux autres nœuds du site. Garantit la cohérence lecture-après-écriture pour toutes les requêtes client au sein du site.
- **Lecture après nouvelle écriture** : Garantit la cohérence en lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et des

garanties de protection des données. Recommandé dans la plupart des cas.

- **Disponible** : Garantit la cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement en cas de besoin (par exemple, pour un compartiment contenant des valeurs de journaux rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.



Avant de choisir une valeur de cohérence, ["lire la description complète de la cohérence"](#). Vous devez comprendre les avantages et les limites avant de modifier la valeur par défaut.

Exemple de la façon dont la cohérence et les règles ILM peuvent interagir

Supposons que vous ayez une grille à trois sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez trois copies de l'objet, une sur le site local et une sur chaque site distant. Utilisez le comportement d'ingestion strict.
- **Cohérence** : Forte et globale (les métadonnées de l'objet sont immédiatement distribuées à plusieurs sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue trois copies de l'objet et distribue les métadonnées à plusieurs sites avant de renvoyer un message de succès au client.

L'objet est intégralement protégé contre toute perte dès la confirmation de son ingestion. Par exemple, si le site local est perdu peu après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur les sites distants. L'objet est entièrement récupérable depuis les autres sites.

Si vous utilisiez la même règle ILM et la cohérence forte des sites, le client pourrait recevoir un message de succès après la réplication des données d'objet sur les sites distants, mais avant la distribution des métadonnées d'objet. 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 après l'ingestion, les métadonnées d'objet sont perdues. L'objet ne peut pas être récupéré.

L'interaction entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'assistance.

Informations connexes

["Exemple 5 : Règles et politique ILM pour le comportement d'ingestion strict"](#)

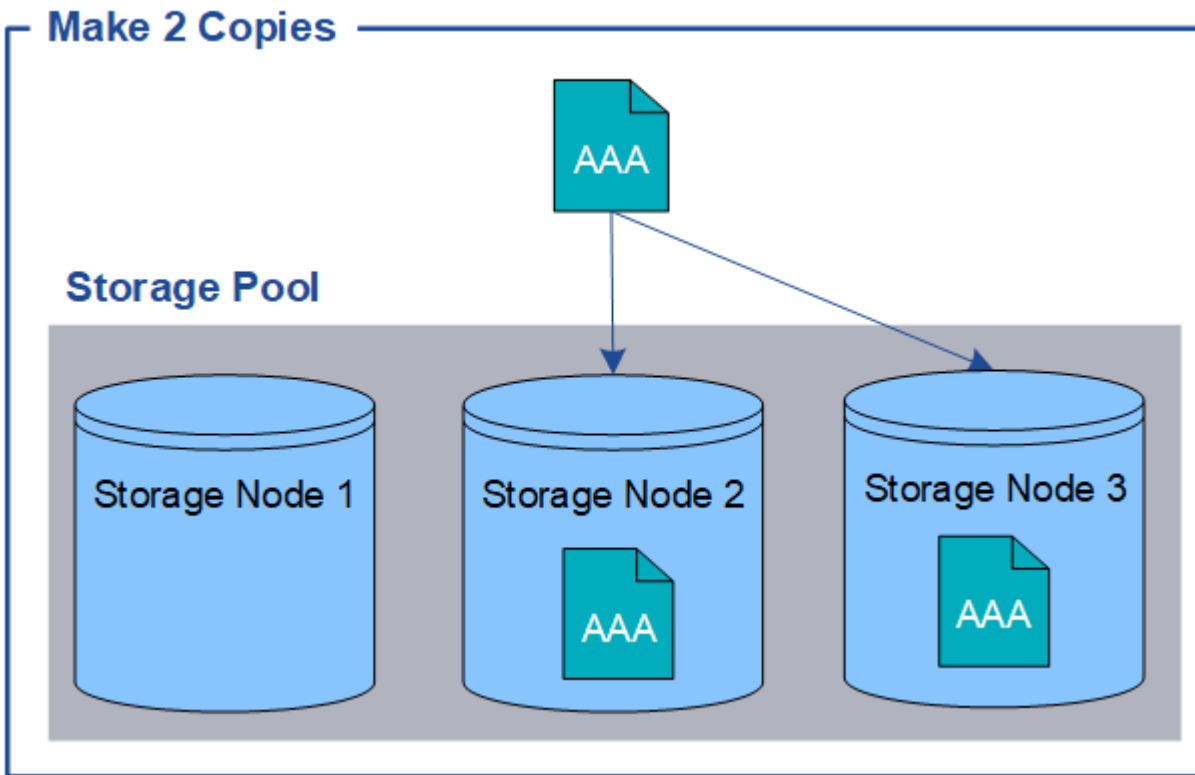
Mode de stockage des objets (réplication ou code d'effacement)

Découvrez la réplication dans StorageGRID

La réplication est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objets (le code d'effacement est l'autre méthode). Lorsque des objets correspondent à une règle ILM qui utilise la réplication, le système crée des copies exactes des données d'objet et les stocke sur les nœuds de stockage.

Lorsque vous configurez une règle ILM pour créer des copies répliquées, vous spécifiez combien de copies doivent être créées, où ces copies doivent être placées et combien de temps les copies doivent être stockées à chaque emplacement.

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



Lorsque StorageGRID associe des objets à cette règle, il crée deux copies de l'objet, plaçant chaque copie sur un nœud de stockage différent dans le pool de stockage. Les deux copies peuvent être placées sur n'importe lesquels des trois nœuds de stockage disponibles. Dans ce cas, la règle a placé les copies de l'objet sur les nœuds de stockage 2 et 3. Parce qu'il y a deux copies, l'objet peut être récupéré si l'un des nœuds du pool de stockage tombe en panne.



StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si votre grid comprend trois nœuds de stockage et que vous créez une règle ILM à 4 copies, seules trois copies seront créées—une copie pour chaque nœud de stockage. L'alerte **ILM placement unachievable** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Informations connexes

- ["Qu'est-ce que le code d'effacement"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Activez la protection contre la perte de site à l'aide de la répllication et du code d'effacement"](#)

Risques de la répllication à copie unique dans StorageGRID

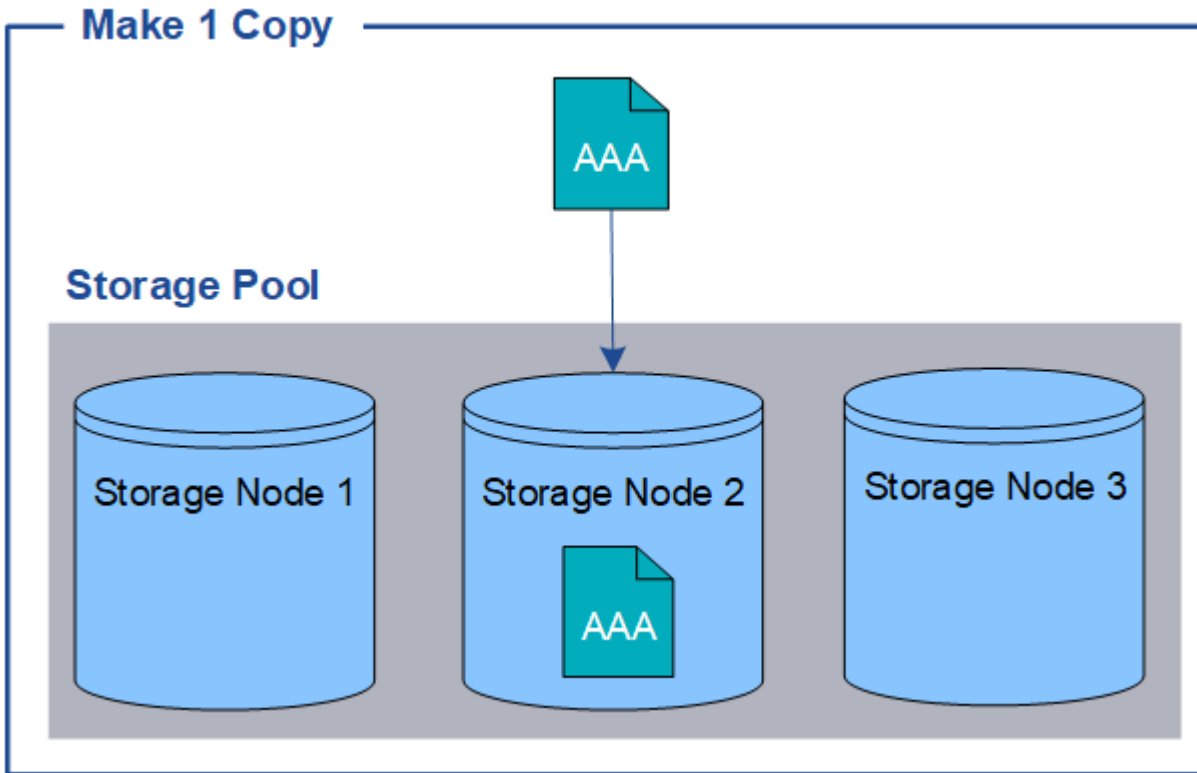
Lors de la création d'une règle ILM pour créer des copies répliquées, vous devez toujours spécifier au moins deux copies pour toute période dans les instructions de placement.



N'utilisez pas de règle ILM qui ne crée qu'une seule copie répliquée pour une période donnée. S'il n'existe qu'une seule copie répliquée d'un objet, cet objet est perdu en cas de défaillance ou d'erreur critique d'un Storage Node. Vous perdez également temporairement l'accès à l'objet lors des procédures de maintenance, telles que les mises à niveau.

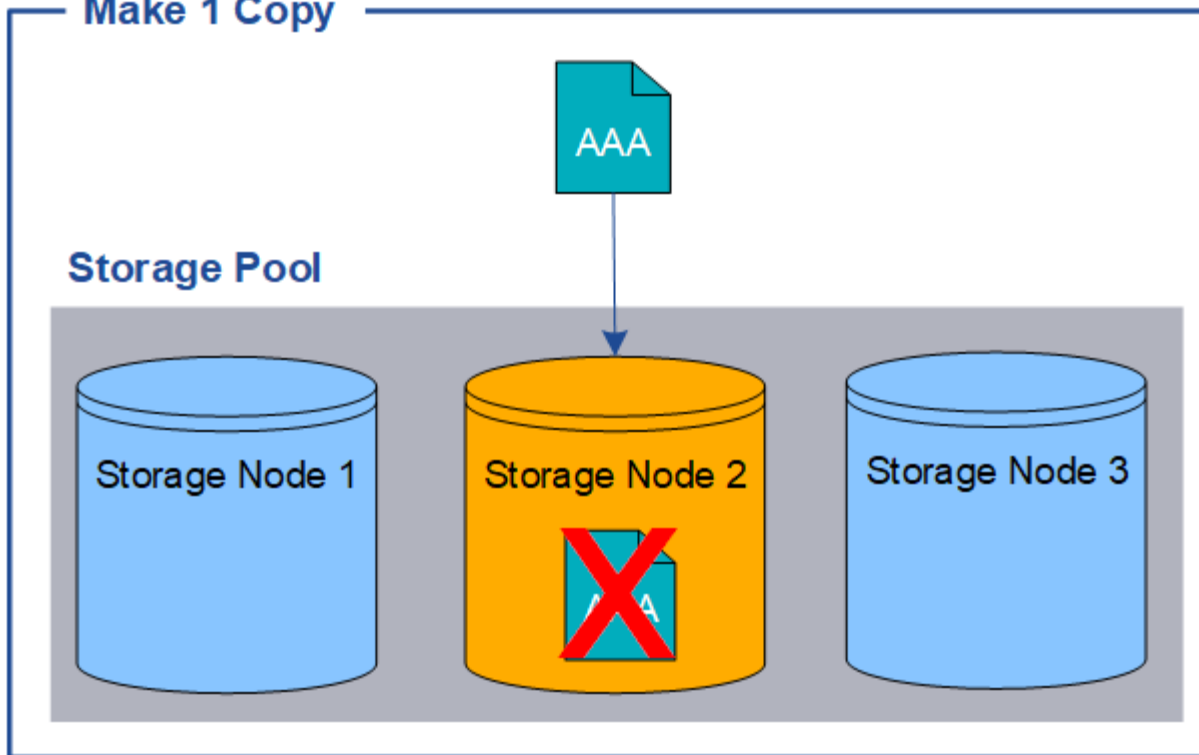
Dans l'exemple suivant, la règle ILM « Make 1 Copy » spécifie qu'une copie répliquée d'un objet doit être

placée dans un pool de stockage contenant trois nœuds de stockage. Lorsqu'un objet correspondant à cette règle est ingéré, StorageGRID place une seule copie sur un seul nœud de stockage.

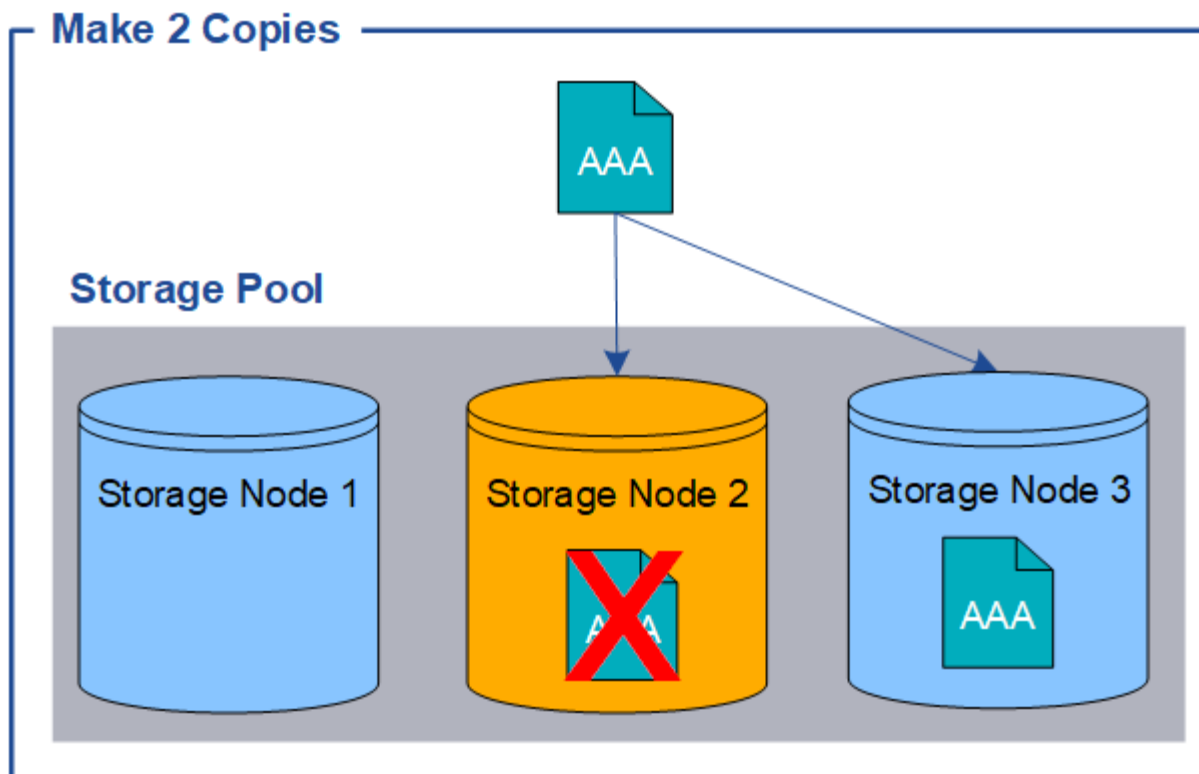


Lorsqu'une règle ILM ne crée qu'une seule copie répliquée d'un objet, l'objet devient inaccessible lorsque le nœud de stockage est indisponible. Dans cet exemple, vous perdrez temporairement l'accès à l'objet AAA chaque fois que le nœud de stockage 2 est hors ligne, par exemple lors d'une mise à niveau ou d'une autre procédure de maintenance. Vous perdrez entièrement l'objet AAA en cas de défaillance du nœud de stockage 2.

Make 1 Copy



Pour éviter de perdre des données d'objet, vous devez toujours créer au moins deux copies de tous les objets que vous souhaitez protéger par réplication. Si deux copies ou plus existent, vous pouvez toujours accéder à l'objet si un Storage Node tombe en panne ou est hors ligne.



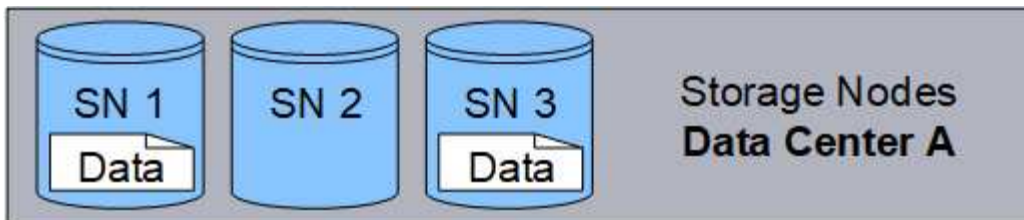
Découvrez le code d'effacement dans StorageGRID

Le code d'effacement est l'une des deux méthodes que StorageGRID utilise pour stocker les données d'objets (la réplication étant l'autre méthode). Lorsque des objets correspondent à une règle ILM utilisant le code d'effacement, ces objets sont découpés en fragments de données, des fragments de parité supplémentaires sont calculés, et chaque fragment est stocké sur un nœud de stockage différent.

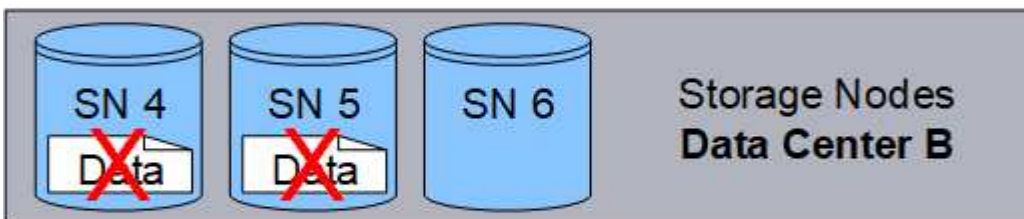
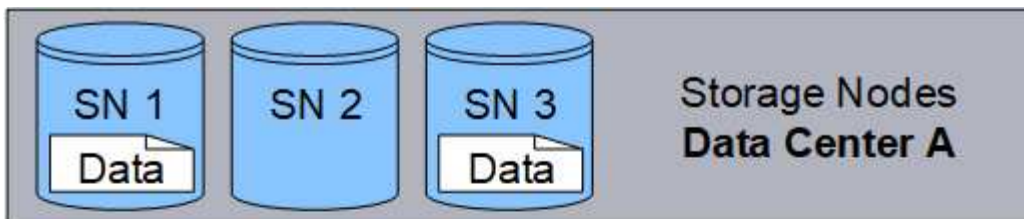
Lorsqu'un objet est accédé, il est reconstitué à partir des fragments stockés. Si un fragment de données ou de parité est corrompu ou perdu, l'algorithme de code d'effacement peut recréer ce fragment à partir d'un sous-ensemble des fragments de données et de parité restants.

Lorsque vous créez des règles ILM, StorageGRID crée des profils de code d'effacement compatibles avec ces règles. Vous pouvez consulter une liste de profils de code d'effacement, "[renommer un profil de code d'effacement](#)", ou "[désactivez un profil de code d'effacement s'il n'est actuellement utilisé dans aucune règle ILM](#)".

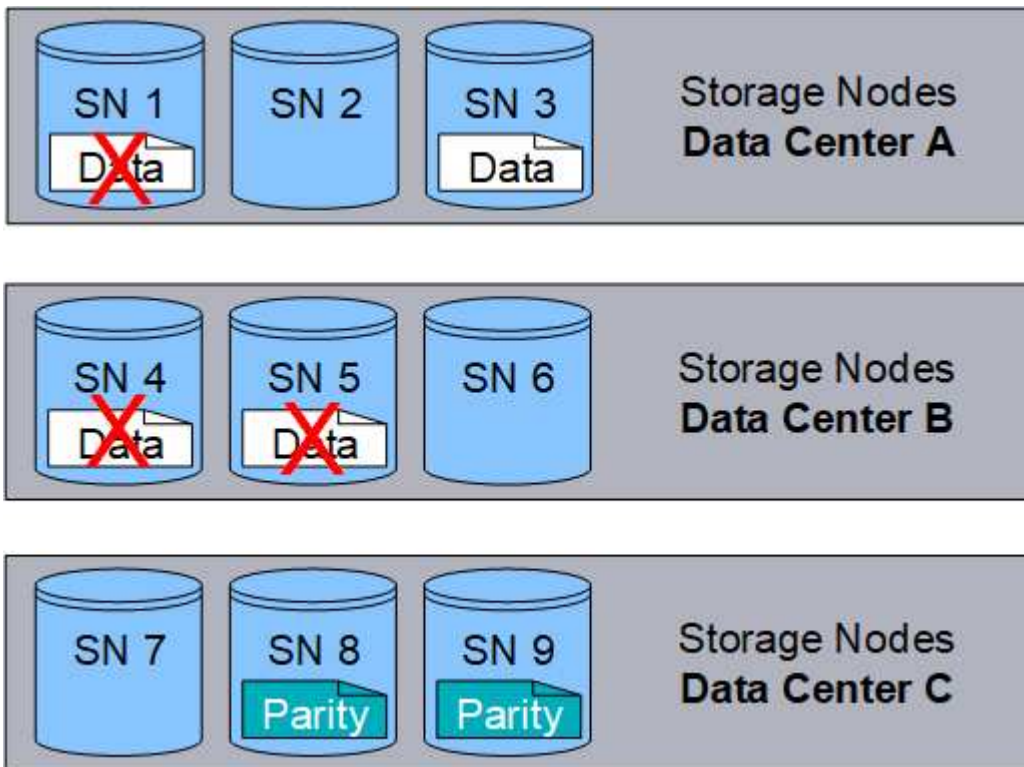
L'exemple suivant illustre l'utilisation d'un algorithme de code d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de code d'effacement 4+2. Chaque objet est divisé en quatre fragments de données égaux, et deux fragments de parité sont calculés à partir des données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



Le schéma de code d'effacement 4+2 peut être configuré de diverses manières. Par exemple, vous pouvez configurer un pool de stockage monosite contenant six Storage Nodes. Pour "[protection contre la perte de site](#)", vous pouvez utiliser un pool de stockage contenant trois sites avec trois Storage Nodes à chaque site. Un objet peut être récupéré tant que quatre des six fragments (données ou parité) restent disponibles. Jusqu'à deux fragments peuvent être perdus sans perte des données de l'objet. Si un site entier est perdu, l'objet peut toujours être récupéré ou réparé, à condition que tous les autres fragments restent accessibles.



Si plus de deux nœuds de stockage sont perdus, l'objet est irrécupérable.



Informations connexes

- ["Qu'est-ce que la réplication"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Que sont les schémas de code d'effacement"](#)
- ["Renommer un profil de codage d'effacement"](#)
- ["Désactivez un profil de codage d'effacement"](#)

Découvrez les schémas de code d'effacement dans StorageGRID

Les schémas de code d'effacement contrôlent le nombre de fragments de données et le nombre de fragments de parité créés pour chaque objet.

Lorsque vous créez ou modifiez une règle ILM, vous sélectionnez un schéma de code d'effacement disponible. StorageGRID crée automatiquement des schémas de code d'effacement en fonction du nombre de nœuds de stockage et de sites composant le pool de stockage que vous prévoyez d'utiliser.

Protection des données

Le système StorageGRID utilise l'algorithme de code d'effacement Reed-Solomon. L'algorithme découpe un objet en k fragments de données et calcule m fragments de parité.

Les $k + m = n$ fragments sont répartis sur n Storage Nodes afin d'assurer la protection des données comme suit :

- Pour récupérer ou réparer un objet, k des fragments sont nécessaires.
- Un objet peut supporter jusqu'à m fragments perdus ou corrompus. Plus la valeur de m est élevée, plus la tolérance aux pannes est grande.

La meilleure protection des données est assurée par le système de code d'effacement présentant la plus grande tolérance aux pannes de nœud ou de volume au sein d'un pool de stockage.

Surcharge de stockage

La surcharge de stockage d'un schéma de code d'effacement se calcule en divisant le nombre de fragments de parité (m) par le nombre de fragments de données (k). Vous pouvez utiliser la surcharge de stockage pour calculer combien d'espace disque chaque objet codé par effacement nécessite :

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Par exemple, si vous stockez un objet de 10 Mo en utilisant le schéma 4+2 (qui induit une surcharge de stockage de 50 %), cet objet occupe 15 Mo de stockage en grid. Si vous stockez le même objet de 10 Mo en utilisant le schéma 6+2 (qui induit une surcharge de stockage de 33 %), il occupe environ 13,3 Mo.

Sélectionnez le schéma de code d'effacement présentant la valeur totale la plus faible $k+m$ qui répond à vos besoins. Les schémas de code d'effacement avec un nombre réduit de fragments sont plus efficaces en termes de calcul parce que :

- Moins de fragments sont créés et distribués (ou récupérés) par objet
- Ils affichent de meilleures performances car la taille des fragments est plus grande
- Ils peuvent nécessiter l'ajout de moins de nœuds dans un ["extension lorsque davantage de stockage est nécessaire"](#)

Lignes directrices pour les pools de stockage

Lors de la sélection du pool de stockage à utiliser pour une règle qui créera une copie à code d'effacement, suivez les instructions suivantes concernant les pools de stockage :

- Le pool de stockage doit inclure trois sites ou plus, ou exactement un seul site.



Vous ne pouvez pas utiliser le code d'effacement si le pool de stockage comprend deux sites.

- [Schémas de code d'effacement pour les pools de stockage contenant trois sites ou plus](#)
- [Schémas de code d'effacement pour les pools de stockage à site unique](#)
- N'utilisez pas un pool de stockage qui inclut le site All Sites.
- Le pool de stockage doit comprendre au moins $k+m + 1$ nœuds de stockage capables de stocker des données d'objets.



Lors de l'installation, les nœuds de stockage peuvent être configurés pour contenir à la fois les données et les métadonnées des objets (nœud de stockage « combiné »), uniquement les métadonnées des objets ou uniquement les données des objets. Pour plus d'informations, consultez ["Types de nœuds de stockage"](#).

Le nombre minimal de nœuds de stockage requis est $k+m$. Toutefois, disposer d'au moins un nœud de stockage supplémentaire peut contribuer à prévenir les échecs d'ingestion ou les retards ILM si un nœud de stockage requis est temporairement indisponible.

Schémas de code d'effacement pour les pools de stockage contenant trois sites ou plus

Le tableau suivant décrit les schémas de code d'effacement actuellement pris en charge par StorageGRID pour les pools de stockage comprenant trois sites ou plus. Tous ces schémas assurent une protection contre la perte d'un site. Un site peut être perdu et l'objet restera accessible.

Pour les schémas de code d'effacement qui assurent une protection contre la perte de site, le nombre recommandé de Storage Nodes dans le pool de stockage est supérieur $k+m + 1$ parce que chaque site nécessite un minimum de trois Storage Nodes.

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 du site ?	Surcharge de stockage
4+2	3	3	9	Oui	50%
6+2	4	3	12	Oui	33%
8+2	5	3	15	Oui	25%
6+3	3	4	12	Oui	50%
9+3	4	4	16	Oui	33%
2+1	3	3	9	Oui	50%
4+1	5	3	15	Oui	25%
6+1	7	3	21	Oui	17%
7+5	3	5	15	Oui	71%



StorageGRID requiert au minimum trois nœuds de stockage par site. Pour utiliser le schéma 7+5, chaque site nécessite au minimum quatre nœuds de stockage. L'utilisation de cinq nœuds de stockage par site est recommandée.

Lors du choix d'un système de code d'effacement assurant la protection d'un site, il convient de prendre en compte l'importance relative des facteurs suivants :

- **Nombre de fragments** : Les performances et la flexibilité d'expansion sont généralement meilleures lorsque le nombre total de fragments est plus faible.
- **Tolérance aux pannes** : La tolérance aux pannes est accrue par un plus grand nombre de segments de parité (c'est-à-dire lorsque m a une valeur plus élevée.)
- **Trafic réseau** : Lors de la récupération après une panne, l'utilisation d'un schéma avec plus de fragments (c'est-à-dire un total plus élevé pour $k+m$) génère plus de trafic réseau.
- **Surcharge de stockage** : Les schémas avec une surcharge plus élevée nécessitent plus d'espace de stockage par objet.

Par exemple, pour choisir entre un schéma 4+2 et un schéma 6+3 (qui présentent tous deux une surcharge de stockage de 50 %), sélectionnez le schéma 6+3 si une tolérance aux pannes supplémentaire est requise. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées. Si tous les autres facteurs sont égaux, sélectionnez le schéma 4+2 car il présente un nombre total de fragments inférieur.



Si vous n’êtes pas sûr du schéma à utiliser, sélectionnez 4+2 ou 6+3, ou contactez le support technique.

Schémas de code d’effacement pour les pools de stockage à site unique

Un pool de stockage à site unique prend en charge tous les schémas de code d’effacement définis pour trois sites ou plus, à condition que le site dispose de suffisamment de nœuds de stockage.

Le nombre minimal de nœuds de stockage requis est $k+m$, mais il est recommandé d’utiliser un pool de stockage avec $k+m +1$ nœuds de stockage. Par exemple, le schéma de code d’effacement 2+1 nécessite un pool de stockage avec un minimum de trois nœuds de stockage, mais il est recommandé d’en utiliser quatre.

Schéma de code d’effacement ($k+m$)	Nombre minimal de nœuds de stockage	Nombre recommandé de nœuds de stockage	Surcharge de stockage
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Avantages, inconvénients et exigences du code d’effacement dans StorageGRID

Avant de décider d’utiliser la réplication ou le code d’effacement pour protéger les données d’objets contre la perte, vous devez comprendre les avantages, les inconvénients et les exigences du code d’effacement.

Avantages du code d’effacement

Comparé à la réplication, le code d’effacement offre une fiabilité, une disponibilité et une efficacité de stockage améliorées.

- **Fiabilité** : Mesurée par le nombre de pannes simultanées pouvant être supportées sans perte de données.
 - Réplication : Plusieurs copies identiques d'un même objet sont stockées sur différents nœuds et sites.
 - Code d'effacement : un objet est encodé en fragments de données et de parité, puis distribué sur plusieurs nœuds et sites. Cette dispersion assure la protection contre les pannes de sites et de nœuds.
- **Disponibilité** : Capacité à accéder aux objets en cas de panne ou d'inaccessibilité des nœuds de stockage. Comparé à la réplication, le code d'effacement offre une disponibilité accrue à coût de stockage équivalent.
- **Efficacité de stockage** : À disponibilité et fiabilité égales, les objets à code d'effacement utilisent moins d'espace disque que les objets répliqués. Par exemple, un objet de 10 Mo répliqué sur deux sites consomme 20 Mo d'espace disque (deux copies), tandis qu'un objet à code d'effacement réparti sur trois sites avec un schéma de code d'effacement 6+3 ne consomme que 15 Mo d'espace disque.



L'espace disque pour les objets à code d'effacement est calculé comme la taille de l'objet plus la surcharge de stockage. Le pourcentage de surcharge de stockage correspond au nombre de fragments de parité divisé par le nombre de fragments de données.

Inconvénients du code d'effacement

Comparé à la réplication, le code d'effacement présente les inconvénients suivants :

- Il est recommandé d'augmenter le nombre de nœuds de stockage et de sites, en fonction du schéma de code d'effacement. En revanche, si vous répliquez les données d'objet, vous n'avez besoin que d'un seul nœud de stockage pour chaque copie. Voir ["Schémas de code d'effacement pour les pools de stockage contenant trois sites ou plus"](#) et ["Schémas de code d'effacement pour les pools de stockage à site unique"](#).
- Augmentation du coût et de la complexité des extensions de stockage. Pour étendre un déploiement utilisant la réplication, vous ajoutez de la capacité de stockage à chaque emplacement où des copies d'objets sont effectuées. Pour étendre un déploiement utilisant le code d'effacement, vous devez tenir compte à la fois du schéma de code d'effacement utilisé et du taux de remplissage des nœuds de stockage existants. Par exemple, si vous attendez que les nœuds existants soient remplis à 100 %, vous devez ajouter au moins $k+m$ nœuds de stockage, mais si vous effectuez l'extension lorsque les nœuds existants sont remplis à 70 %, vous pouvez ajouter deux nœuds par site et optimiser ainsi la capacité de stockage utilisable. Pour plus d'informations, consultez ["Ajouter de la capacité de stockage pour les objets à code d'effacement"](#).
- L'utilisation du code d'effacement sur des sites géographiquement distribués entraîne une augmentation de la latence de récupération. Les fragments d'un objet codé par effacement et distribués sur des sites distants mettent plus de temps à être récupérés via des connexions WAN que ceux d'un objet répliqué et disponible localement (sur le même site auquel le client se connecte).
- Lorsque vous utilisez le code d'effacement sur des sites géographiquement répartis, le trafic réseau WAN est plus important pour les récupérations et les réparations, en particulier pour les objets fréquemment récupérés ou pour les réparations d'objets via des connexions réseau WAN.
- Lorsque vous utilisez le code d'effacement entre plusieurs sites, le débit maximal d'objets diminue fortement à mesure que la latence réseau entre les sites augmente. Cette diminution est due à une baisse du débit du réseau TCP, ce qui affecte la rapidité avec laquelle le système StorageGRID peut stocker et récupérer les fragments d'objets.
- Utilisation accrue des ressources de calcul.

Quand utiliser le code d'effacement

Utilisez le code d'effacement pour répondre aux exigences suivantes :

- Objets de taille supérieure à 1 Mo.



Le code d'effacement est idéal pour les objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets de moins de 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

- Stockage à long terme ou à froid pour les contenus rarement consultés.
- Haute disponibilité et fiabilité des données.
- Protection contre les défaillances complètes de sites et de nœuds.
- Efficacité du stockage.
- Déploiements sur un seul site nécessitant une protection efficace des données avec une seule copie à code d'effacement plutôt que plusieurs copies répliquées.
- Déploiements multisites où la latence inter-sites est inférieure à 100 ms.

Comment StorageGRID détermine la conservation des objets

StorageGRID offre aux administrateurs de la grille et aux utilisateurs individuels la possibilité de spécifier la durée de conservation des objets. En règle générale, toute instruction de conservation fournie par un utilisateur locataire prévaut sur les instructions de conservation fournies par l'administrateur de la grille.

Comment les utilisateurs locataires contrôlent la conservation des objets

Les utilisateurs locataires peuvent utiliser ces méthodes pour contrôler la durée de stockage de leurs objets dans StorageGRID :

- Si le paramètre global de verrouillage des objets S3 est activé pour la grille, les utilisateurs du locataire S3 peuvent créer des compartiments avec le verrouillage des objets S3 activé, puis sélectionner une **période de rétention par défaut** pour chaque compartiment.
- Si le paramètre global de S3 Object Lock est activé pour la grille, les utilisateurs locataires S3 peuvent créer des compartiments avec S3 Object Lock activé, puis utiliser l'API REST S3 pour spécifier retain-until-date et les paramètres de legal hold pour chaque version d'objet ajoutée à ce compartiment.
 - Une version d'objet faisant l'objet d'une restriction légale ne peut être supprimée par aucune méthode.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut être supprimée par aucune méthode.
 - Les objets contenus dans les compartiments avec S3 Object Lock activé sont conservés « indéfiniment » par ILM. Cependant, une fois la date limite de conservation atteinte, une version de l'objet peut être supprimée par une requête client ou à l'expiration du cycle de vie du compartiment. Voir "[Gérez les objets avec S3 Object Lock](#)".
- Les utilisateurs locataires S3 peuvent ajouter une configuration de cycle de vie à leurs compartiments qui spécifie une action d'expiration. Si un cycle de vie de compartiment existe, StorageGRID stocke un objet jusqu'à la date ou au nombre de jours spécifié dans l'action d'expiration, à moins que le client ne supprime l'objet en premier. Voir "[Créer une configuration de cycle de vie S3](#)".
- Un client S3 peut émettre une requête de suppression d'objet. StorageGRID privilégie toujours les requêtes de suppression client par rapport au cycle de vie du compartiment S3 ou à l'ILM pour déterminer s'il convient de supprimer ou de conserver un objet.

Comment les administrateurs de grille contrôlent la conservation des objets

Les administrateurs de grille peuvent utiliser ces méthodes pour contrôler la conservation des objets :

- Définissez une période de rétention maximale pour le verrouillage d'objet S3 pour chaque locataire. Ensuite, les utilisateurs locataires peuvent définir une période de rétention par défaut pour chacun de leurs compartiments. La période de rétention maximale est également appliquée à tout nouvel objet ingéré pour ce compartiment (date de conservation de l'objet).
- Créez des instructions de placement ILM pour contrôler la durée de stockage des objets. Lorsqu'un objet correspond à une règle ILM, StorageGRID stocke ces objets jusqu'à ce que la dernière période définie dans la règle ILM soit écoulée. Les objets sont conservés indéfiniment si « forever » est spécifié dans les instructions de placement.
- Peu importe qui contrôle la durée de conservation des objets, les paramètres ILM contrôlent les types de copies d'objets (répliquées ou à code d'effacement) qui sont stockées et l'emplacement de ces copies (Storage Nodes ou Cloud Storage Pools).

Interaction entre le cycle de vie d'un compartiment S3 et ILM

Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration de ce cycle de vie prévalent sur la stratégie ILM pour les objets correspondant au filtre de cycle de vie. Par conséquent, un objet peut rester sur la grille même après l'expiration des instructions ILM relatives à son placement.

Exemples de rétention d'objets

Pour mieux comprendre les interactions entre S3 Object Lock, les paramètres du cycle de vie du compartiment, les demandes de suppression du client et ILM, considérez les exemples suivants.

Exemple 1 : Le cycle de vie d'un compartiment S3 conserve les objets plus longtemps que l'ILM

ILM

Conservez deux exemplaires pendant 1 an (365 jours)

Cycle de vie du bucket

Expirer les objets dans 2 ans (730 jours)

Résultat

StorageGRID conserve l'objet pendant 730 jours. StorageGRID utilise les paramètres de cycle de vie du compartiment pour déterminer s'il convient de supprimer ou de conserver un objet.



Si le cycle de vie du compartiment spécifie que les objets doivent être conservés plus longtemps que prévu par ILM, StorageGRID continue d'utiliser les instructions de placement d'ILM pour déterminer le nombre et le type de copies à stocker. Dans cet exemple, deux copies de l'objet continueront d'être stockées dans StorageGRID du 366e au 730e jour.

Exemple 2 : Le cycle de vie d'un compartiment S3 expire les objets avant l'ILM

ILM

Conservez deux exemplaires pendant 2 ans (730 jours)

Cycle de vie du bucket

Expirer les objets dans 1 an (365 jours)

Résultat

StorageGRID supprime les deux copies de l'objet après le jour 365.

Exemple 3 : La suppression côté client remplace le cycle de vie du compartiment et l'ILM

ILM

Stockez deux copies sur les nœuds de stockage « forever »

Cycle de vie du bucket

Expirer les objets dans 2 ans (730 jours)

Demande de suppression du client

Émis le 400e jour

Résultat

StorageGRID supprime les deux copies de l'objet le 400e jour en réponse à la demande de suppression du client.

Exemple 4 : Le verrouillage d'objet S3 remplace la requête de suppression du client

Verrouillage d'objet S3

La date limite de conservation pour une version d'objet est le 31 mars 2026. Aucune restriction légale n'est en vigueur.

Règle ILM conforme

Stockez deux copies sur les nœuds de stockage « forever »

Demande de suppression du client

Publié le 31 mars 2024

Résultat

StorageGRID ne supprimera pas la version de l'objet car la date de conservation est encore dans 2 ans.

Comment StorageGRID supprime des objets

StorageGRID peut supprimer des objets soit directement suite à une requête client, soit automatiquement à l'expiration du cycle de vie d'un compartiment S3 ou conformément aux exigences de la politique ILM. Comprendre les différentes méthodes de suppression d'objets et la manière dont StorageGRID traite les demandes de suppression peut vous aider à gérer les objets plus efficacement.

StorageGRID peut utiliser l'une des deux méthodes pour supprimer des objets :

- Suppression synchrone : lorsqu'un client StorageGRID effectue une requête de suppression, toutes les copies d'objets sont immédiatement supprimées. Le client est informé que la suppression a réussi après que les copies ont été supprimées.
- Les objets sont mis en file d'attente pour suppression : lorsqu'une demande de suppression est reçue par StorageGRID, l'objet est mis en file d'attente et le client est immédiatement informé que la suppression a réussi. Les copies de l'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, minimise les risques d’accumulation de suppressions et libère l’espace le plus rapidement possible.

Le tableau récapitule les cas où StorageGRID utilise chaque méthode.

Méthode de suppression	Lorsqu’il est utilisé
Les objets sont mis en file d’attente pour suppression	Lorsque l’une des conditions suivantes est vraie : • La suppression automatique de l’objet a été déclenchée par l’un des événements suivants : ◦ La date d’expiration ou le nombre de jours dans la configuration du cycle de vie d’un compartiment S3 est atteinte. ◦ La dernière période spécifiée dans une règle ILM s’écoule. Remarque : Les objets d’un compartiment pour lequel le verrouillage d’objets S3 est activé ne peuvent pas être supprimés s’ils font l’objet d’une conservation légale ou si une date de conservation a été spécifiée mais n’a pas encore été atteinte. • <code>\${post_edited_translations.segment}</code> ◦ <code>\${post_edited_translations.segment}</code> ◦ Les files d’attente de suppression en arrière-plan sont inactives.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code> • <code>\${post_edited_translations.segment}</code> • <code>\${post_edited_translations.segment}</code>

Lorsque les clients S3 effectuent des requêtes de suppression, StorageGRID commence par ajouter les objets à la file d’attente de suppression. Il passe ensuite à l’exécution de la suppression synchrone. S’assurer que la file d’attente de suppression en arrière-plan contient des objets à traiter permet à StorageGRID de traiter les suppressions plus efficacement, en particulier pour les clients à faible simultanéité, tout en contribuant à éviter les retards de suppression des clients.

Temps nécessaire pour supprimer les objets

`${post_edited_translations.segment}`

- Lorsque StorageGRID effectue une suppression synchrone, il peut falloir jusqu’à 30 secondes à StorageGRID pour renvoyer un résultat au client. Cela signifie que la suppression peut sembler plus lente, même si les copies sont en réalité supprimées plus rapidement que lorsque StorageGRID met les objets en file d’attente pour suppression.
- Si vous surveillez attentivement les performances de suppression lors d’une suppression en masse, vous remarquerez peut-être que le débit de suppression semble ralentir après la suppression d’un certain nombre d’objets. Ce changement se produit lorsque StorageGRID passe de la mise en file d’attente des objets à supprimer à une suppression synchrone. Cette réduction apparente du débit de suppression ne signifie pas que les copies d’objets sont supprimées plus lentement. Au contraire, cela indique qu’en moyenne, l’espace est désormais libéré plus rapidement.

Si vous supprimez un grand nombre d’objets et que votre priorité est de libérer rapidement de l’espace,

envisagez d'utiliser une requête client pour supprimer les objets plutôt que de les supprimer à l'aide de l'ILM ou d'autres méthodes. En général, l'espace est libéré plus rapidement lorsque la suppression est effectuée par les clients, car StorageGRID peut utiliser la suppression synchrone.

Le temps nécessaire pour libérer de l'espace après la suppression d'un objet dépend de plusieurs facteurs :

- `#{post_edited_translations.segment}`
- D'autres facteurs tels que le nombre d'objets dans la grille ou la disponibilité des ressources de la grille lorsque des copies d'objets sont mises en file d'attente pour suppression (pour les suppressions côté client et d'autres méthodes).

`#{post_edited_translations.segment}`

Lorsque le versionnage est activé pour un compartiment S3, StorageGRID suit le comportement d'Amazon S3 lorsqu'il répond aux demandes de suppression, que ces demandes proviennent d'un client S3, de l'expiration du cycle de vie d'un compartiment S3 ou des exigences de la politique ILM.

Lorsque les objets sont versionnés, les requêtes de suppression d'objet ne suppriment pas la version actuelle de l'objet et ne libèrent pas d'espace. À la place, une requête de suppression d'objet crée un marqueur de suppression de zéro octet en tant que version actuelle de l'objet, ce qui rend la version précédente de l'objet "non actuelle". Un marqueur de suppression d'objet devient un marqueur de suppression d'objet expiré lorsqu'il s'agit de la version actuelle et qu'il n'existe aucune version non actuelle.

Même si l'objet n'a pas été supprimé, StorageGRID se comporte comme si la version actuelle de l'objet n'était plus disponible. Les requêtes adressées à cet objet renvoient 404 Not Found. Toutefois, comme les données d'objet non actuelles n'ont pas été supprimées, les requêtes qui spécifient une version non actuelle de l'objet peuvent réussir.

Si un client supprime une version d'objet avec un ID de version d'un "bucket de branche" compartiment de branche, StorageGRID masque l'existence de cette version d'objet mais ne crée pas d'indicateur de suppression dans le compartiment de branche. Si un client supprime un objet sans ID de version d'un compartiment de branche, StorageGRID crée un indicateur de suppression dans le compartiment de branche conformément au comportement standard de S3.

Pour libérer de l'espace lors de la suppression d'objets versionnés ou pour supprimer les marqueurs de suppression, utilisez l'une des méthodes suivantes :

- **Requête client S3** : Spécifiez l'ID de version de l'objet dans la requête S3 DELETE Object (`DELETE /object?versionId=ID`). Notez que cette requête supprime uniquement les copies de l'objet pour la version spécifiée (les autres versions continuent d'occuper de l'espace).
- **Cycle de vie des buckets** : Utilisez l' `NoncurrentVersionExpiration` action dans la configuration du cycle de vie du bucket. Lorsque le nombre de `NoncurrentDays` spécifié est atteint, StorageGRID supprime définitivement toutes les copies des versions d'objets non actuelles. Ces versions d'objets ne peuvent pas être récupérées.

L' `NewerNoncurrentVersions` action dans la configuration du cycle de vie du compartiment spécifie le nombre de versions non actuelles conservées dans un compartiment S3 versionné. S'il existe plus de versions non actuelles que ce que `NewerNoncurrentVersions` spécifie, StorageGRID supprime les versions les plus anciennes lorsque la valeur `NoncurrentDays` est atteinte. Le seuil `NewerNoncurrentVersions` remplace les règles de cycle de vie fournies par ILM, ce qui signifie qu'un objet non actuel dont la version se trouve dans la limite du seuil `NewerNoncurrentVersions` est conservé si ILM demande sa suppression.

Pour supprimer les marqueurs de suppression d'objet expirés, utilisez l'action `Expiration` avec l'une des

balises suivantes : `ExpiredObjectDeleteMarker`, `Days` ou `Date`.

- **ILM** : "[Cloner une politique active](#)" et ajoutez deux règles ILM à la nouvelle politique :
 - Première règle : utilisez « Heure non actuelle » comme heure de référence pour faire correspondre les versions non actuelles de l'objet. Dans "[Étape 1 \(Saisie des détails\) de l'assistant Créer une règle ILM](#)", sélectionnez **Oui** pour la question : « Appliquer cette règle uniquement aux anciennes versions de l'objet (dans les compartiments S3 avec le versionnage activé) ? »
 - Deuxième règle : Utilisez la **Heure d'ingestion** pour qu'elle corresponde à la version actuelle. La règle « Heure non actuelle » doit figurer dans la stratégie au-dessus de la règle **Heure d'ingestion**.

Pour supprimer les marqueurs de suppression d'objets expirés, utilisez une règle de **Ingest time** correspondant aux marqueurs de suppression actuels. Les marqueurs de suppression ne sont supprimés que lorsqu'une **Time period** de **Days** s'est écoulée et que le marqueur de suppression actuel a expiré (il n'existe pas de versions non actuelles).

- **Supprimer des objets dans un compartiment** : Utilisez le gestionnaire de locataires pour "[supprimer toutes les versions d'objet](#)" supprimer des objets, y compris les marqueurs de suppression, d'un compartiment.

Lorsqu'un objet versionné est supprimé, StorageGRID crée un marqueur de suppression de zéro octet correspondant à la version actuelle de l'objet. Tous les objets et marqueurs de suppression doivent être supprimés avant qu'un compartiment versionné puisse être supprimé.

- Les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure ne peuvent être supprimés que par le biais de requêtes client S3, ils ne sont pas supprimés par ILM, les règles de cycle de vie du compartiment ou les opérations de suppression d'objets dans le compartiment.
- Les marqueurs de suppression d'un compartiment créé dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés par ILM, les règles de cycle de vie du compartiment, les opérations de suppression d'objets dans le compartiment ou une suppression explicite du client S3.

Informations connexes

- "[Utilisez l'API REST S3](#)"
- "[Exemple 4 : Règles et politique ILM pour les objets versionnés S3](#)"

Créez et attribuez des niveaux de stockage dans StorageGRID

Les niveaux de stockage identifient le type de stockage utilisé par un nœud de stockage. Vous pouvez créer des niveaux de stockage si vous souhaitez que les règles ILM placent certains objets sur certains nœuds de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

À propos de cette tâche

Lors de la première installation de StorageGRID, le niveau de stockage **par défaut** est automatiquement attribué à chaque nœud de stockage de votre système. Selon vos besoins, vous pouvez également définir des niveaux de stockage personnalisés et les attribuer à différents nœuds de stockage.

L'utilisation de niveaux de stockage personnalisés vous permet de créer des pools de stockage ILM contenant uniquement un type spécifique de nœud de stockage. Par exemple, vous pouvez souhaiter que certains objets

soient stockés sur vos nœuds de stockage les plus rapides, tels que les appliances de stockage 100 % Flash StorageGRID.



Il est impossible d'attribuer une note de stockage aux nœuds de stockage contenant uniquement des métadonnées. Pour plus d'informations, veuillez consulter "[Types de nœuds de stockage](#)".

Si le niveau de stockage n'est pas un critère important (par exemple, si tous les nœuds de stockage sont identiques), vous pouvez ignorer cette procédure et utiliser la sélection **inclut tous les niveaux de stockage** pour le niveau de stockage lorsque vous "[créer des pools de stockage](#)". L'utilisation de cette sélection garantit que le pool de stockage inclura chaque nœud de stockage du site, quel que soit son niveau de stockage.



Ne créez pas plus de niveaux de stockage que nécessaire. Par exemple, ne créez pas un niveau de stockage pour chaque Storage Node. Attribuez plutôt chaque niveau de stockage à deux nœuds ou plus. Les niveaux de stockage attribués à un seul nœud peuvent entraîner des retards ILM si ce nœud devient indisponible.

Étapes

1. Sélectionnez **ILM > Niveaux de stockage**.
2. Définir des niveaux de stockage personnalisés :
 - a. Pour chaque niveau de stockage personnalisé que vous souhaitez ajouter, sélectionnez **Insérer**  pour ajouter une ligne.
 - b. Saisissez une étiquette descriptive.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Sélectionnez **Appliquer les modifications**.

d. Si vous devez modifier une étiquette enregistrée, sélectionnez **Modifier** et sélectionnez **Appliquer les modifications**.



Vous ne pouvez pas supprimer les classes de stockage.

3. Attribuez de nouveaux niveaux de stockage aux nœuds de stockage :

a. Repérez le nœud de stockage dans la liste LDR et sélectionnez son icône **Modifier** .

b. Sélectionnez le niveau de stockage approprié dans la liste.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



N'attribuez un niveau de stockage à un nœud de stockage donné qu'une seule fois. Un nœud de stockage remis en service après une panne conserve le niveau de stockage précédemment attribué. Ne modifiez pas cette attribution après l'activation de la stratégie ILM. Si l'attribution est modifiée, les données sont stockées selon le nouveau niveau de stockage.

a. Sélectionnez **Appliquer les modifications**.

`${post_edited_translations.segment}`

Découvrez les pools de stockage dans StorageGRID

Un pool de stockage est un regroupement logique de nœuds de stockage.

Lors de l'installation de StorageGRID, un pool de stockage par site est automatiquement créé. Vous pouvez configurer des pools de stockage supplémentaires en fonction de vos besoins en stockage.



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir des données d'objet et des métadonnées (nœud de stockage « combiné »), uniquement des métadonnées d'objet ou uniquement des données d'objet. Les nœuds de stockage contenant uniquement des métadonnées ne peuvent pas être utilisés dans des pools de stockage. Pour plus d'informations, reportez-vous à "[Types de nœuds de stockage](#)".

Les pools de stockage possèdent deux attributs :

- `${post_edited_translations.segment}`
- **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 et le type de stockage utilisé. Lors de la configuration des règles ILM pour la réplication, vous sélectionnez un ou plusieurs pools de stockage.

Directives de configuration des pools de stockage dans StorageGRID

Configurez et utilisez des pools de stockage pour vous protéger contre la perte de données en répartissant les données sur plusieurs sites. Les copies répliquées et les copies à code d'effacement nécessitent des configurations de pool de stockage différentes.

Voir ["Exemples d'activation de la protection contre la perte de site à l'aide de la réplication et du code d'effacement"](#).

Directives pour tous les pools de stockage

- Simplifiez au maximum la configuration de vos pools de stockage. Ne créez pas plus de pools de stockage que nécessaire.
- Créez des pools de stockage comportant autant de nœuds que possible. Chaque pool de stockage doit contenir deux nœuds ou plus. Un pool de stockage avec un nombre insuffisant de nœuds peut entraîner des retards ILM si un nœud devient indisponible.
- Évitez de créer ou d'utiliser des pools de stockage qui se chevauchent (contenant un ou plusieurs des mêmes nœuds). Si des pools de stockage se chevauchent, il est possible que plusieurs copies des données d'objet soient enregistrées sur le même nœud.
- En règle générale, n'utilisez pas le pool de stockage « All Storage Nodes » (StorageGRID 11.6 et versions antérieures) ni le site « All Sites ». Ces éléments sont automatiquement mis à jour pour inclure tout nouveau site que vous ajoutez lors d'une extension, ce qui pourrait ne pas être le comportement souhaité.

Directives relatives aux pools de stockage utilisés pour les copies répliquées

- Pour la protection contre la perte de site à l'aide de ["réplication"](#), spécifiez un ou plusieurs pools de stockage spécifiques au site dans le ["Instructions de placement pour chaque règle ILM"](#).

Un pool de stockage est automatiquement créé pour chaque site lors de l'installation de StorageGRID.

L'utilisation d'un pool de stockage pour chaque site garantit que les copies d'objets répliquées sont placées exactement là où vous vous y attendez (par exemple, une copie de chaque objet sur chaque site pour la protection contre la perte de site).

- Si vous ajoutez un site dans une extension, créez un nouveau pool de stockage contenant uniquement le nouveau site. Ensuite, ["mettre à jour les règles ILM"](#) pour contrôler quels objets sont stockés sur le nouveau site.
- Si le nombre de copies est inférieur au nombre de pools de stockage, le système répartit les copies afin d'équilibrer l'utilisation du disque entre les pools.
- Si les pools de stockage se chevauchent (contiennent les mêmes Storage Nodes), toutes les copies de l'objet risquent d'être enregistrées sur un seul site. Vous devez vous assurer que les pools de stockage sélectionnés ne contiennent pas les mêmes Storage Nodes.

Directives relatives aux pools de stockage utilisés pour les copies à code d'effacement

- Pour la protection contre la perte de sites à l'aide de ["code d'effacement"](#), créez des pools de stockage composés d'au moins trois sites. Si un pool de stockage comprend uniquement deux sites, vous ne pouvez pas utiliser ce pool de stockage pour le code d'effacement. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage comportant deux sites.
- Le nombre de nœuds de stockage et de sites contenus dans le pool de stockage détermine quels ["schémas de code d'effacement"](#) sont disponibles.

- Dans la mesure du possible, un pool de stockage devrait comporter plus de nœuds de stockage que le nombre minimal requis par le schéma de code d'effacement que vous sélectionnez. Par exemple, si vous utilisez un schéma de code d'effacement 6+3, vous devez disposer d'au moins neuf nœuds de stockage. Cependant, il est recommandé d'avoir au moins un nœud de stockage supplémentaire par site.
- Répartissez les nœuds de stockage sur les sites de manière aussi uniforme que possible. Par exemple, pour prendre en charge un schéma de code d'effacement 6+3, configurez un pool de stockage comprenant au moins trois nœuds de stockage répartis sur trois sites.
- Si vos exigences en matière de débit sont élevées, l'utilisation d'un pool de stockage incluant plusieurs sites est déconseillée si la latence réseau entre les sites dépasse 100 ms. À mesure que la latence augmente, le taux auquel StorageGRID peut créer, placer et récupérer des fragments d'objets diminue fortement en raison de la baisse du débit du réseau TCP.

La diminution du débit affecte les taux maximaux d'ingestion et de récupération d'objets (lorsque les modes Équilibré ou Strict sont sélectionnés comme comportement d'ingestion) ou peut entraîner des engorgements de la file d'attente ILM (lorsque le mode Double validation est sélectionné comme comportement d'ingestion). Voir "[Comportement d'ingestion des règles ILM](#)".



Si votre grille ne comprend qu'un seul site, vous ne pouvez pas utiliser le pool de stockage All Storage Nodes (StorageGRID 11.6 et versions antérieures) ni le site All Sites dans un profil de code d'effacement. Ce comportement empêche que le profil ne devienne invalide si un deuxième site est ajouté.

Protection contre les pertes de site grâce aux pools de stockage dans StorageGRID

Si votre déploiement StorageGRID comprend plusieurs sites, vous pouvez utiliser la réplication et le code d'effacement avec des pools de stockage correctement configurés pour activer la protection contre la perte de sites.

La réplication et le code d'effacement nécessitent des configurations de pool de stockage différentes :

- Pour utiliser la réplication afin de se prémunir contre les pertes de sites, utilisez les pools de stockage spécifiques à chaque site qui sont automatiquement créés lors de l'installation de StorageGRID. Créez ensuite des règles ILM avec "[instructions de placement](#)" qui spécifient plusieurs pools de stockage afin qu'une copie de chaque objet soit placée sur chaque site.
- Pour utiliser le code d'effacement pour la protection contre la perte de sites, "[créer des pools de stockage composés de plusieurs sites](#)". Créez ensuite des règles ILM qui utilisent un pool de stockage composé de plusieurs sites et de tout schéma de code d'effacement disponible.



Lors de la configuration de votre déploiement StorageGRID pour la protection contre la perte de site, vous devez également prendre en compte les effets de "[options d'ingestion](#)" et "[cohérence](#)".

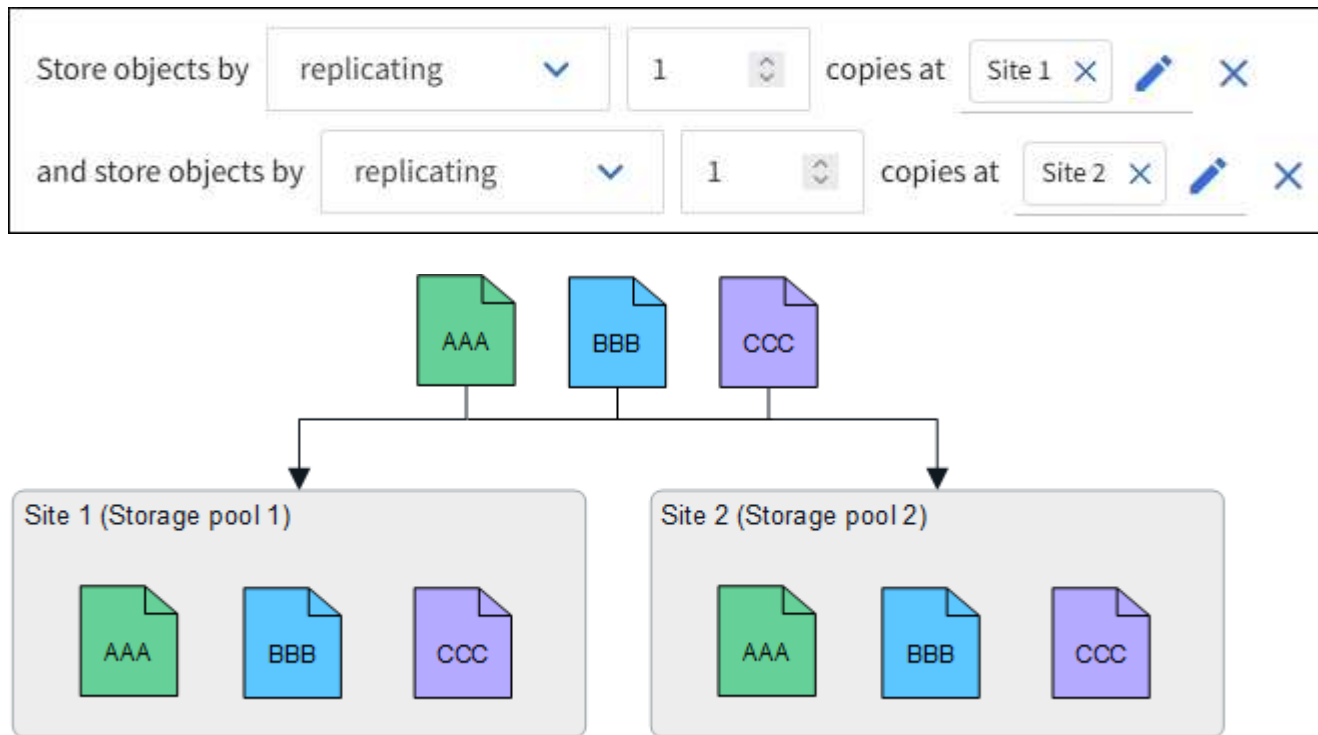
Exemple de réplication

Par défaut, un pool de stockage est créé pour chaque site lors de l'installation de StorageGRID. Le fait de disposer de pools de stockage composés d'un seul site permet de configurer des règles ILM utilisant la réplication pour la protection contre la perte de site. Dans cet exemple :

- Le pool de stockage 1 contient le site 1
- Le pool de stockage 2 contient Site 2

- La règle ILM comporte deux placements :
 - Stockez les objets en répliquant 1 copie sur le site 1
 - Stockez les objets en répliquant 1 copie sur le site 2

Placements des règles ILM :



Si un site est perdu, des copies des objets sont disponibles sur l'autre site.

Exemple de code d'effacement

Le fait de disposer de pools de stockage composés de plusieurs sites par pool de stockage permet de configurer des règles ILM utilisant le code d'effacement pour la protection contre la perte de sites. Dans cet exemple :

- Le pool de stockage 1 contient les sites 1 à 3
- La règle ILM contient un placement : stocker les objets par code d'effacement à l'aide d'un schéma EC 4+2 dans le Storage pool 1, qui contient trois sites

Placements des règles ILM :

Dans cet exemple :

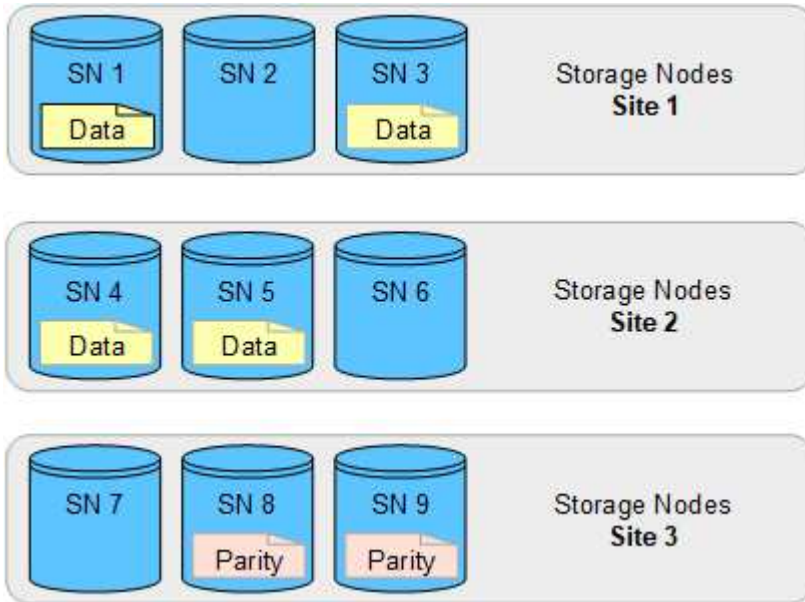
- La règle ILM utilise un schéma de code d'effacement 4+2.
- Chaque objet est découpé en quatre fragments de données égaux, et deux fragments de parité sont calculés à partir des données de l'objet.

- Chacun des six fragments est stocké sur un nœud différent réparti sur trois sites de centres de données afin d'assurer la protection des données en cas de panne de nœud ou de perte de site.

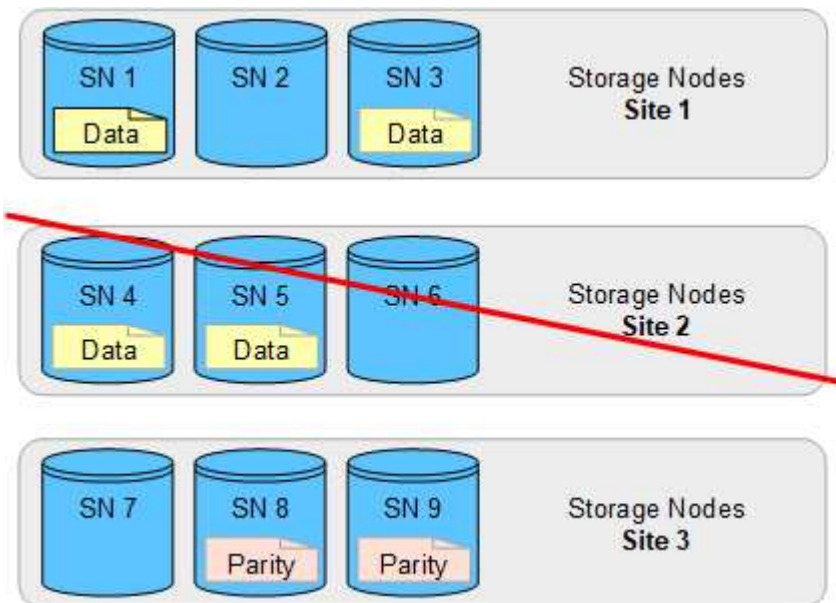


Le code d'effacement est autorisé dans les pools de stockage contenant n'importe quel nombre de sites *sauf* deux sites.

Règle ILM utilisant un schéma de code d'effacement 4+2 :



Si un site est perdu, les données peuvent encore être récupérées :



Créez un pool de stockage dans StorageGRID

Vous créez des pools de stockage pour déterminer où le système StorageGRID stocke les données des objets et le type de stockage utilisé. Chaque pool de stockage comprend un ou plusieurs sites et un ou plusieurs niveaux de stockage.



Lors de l'installation de StorageGRID 12.0 sur une nouvelle grille, des pools de stockage sont automatiquement créés pour chaque site. En revanche, si vous avez initialement installé StorageGRID 11.6 ou une version antérieure, des pools de stockage ne sont pas automatiquement créés pour chaque site.

Si vous souhaitez créer des pools de stockage cloud pour stocker des données d'objets en dehors de votre système StorageGRID, consultez la ["informations sur l'utilisation des Cloud Storage Pools"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez pris connaissance des instructions relatives à la création de pools de stockage.

À propos de cette tâche

Les pools de stockage déterminent où les données d'objets sont stockées. Le nombre de pools de stockage dont vous avez besoin dépend du nombre de sites dans votre grille et du type de copies que vous souhaitez : répliquées ou à code d'effacement.

- Pour la réplication et le code d'effacement sur un seul site, créez un pool de stockage pour chaque site. Par exemple, si vous souhaitez stocker des copies d'objets répliquées sur trois sites, créez trois pools de stockage.
- Pour le code d'effacement sur trois sites ou plus, créez un pool de stockage contenant une entrée pour chaque site. Par exemple, si vous souhaitez appliquer le code d'effacement aux objets sur trois sites, créez un seul pool de stockage.



N'incluez pas le site « 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 stockera des données codées par effacement. Voir [cette étape](#) pour un exemple.

- Si vous disposez de plusieurs niveaux de stockage, ne créez pas un pool de stockage regroupant différents niveaux de stockage sur un même site. Voir la ["Instructions pour la création de pools de stockage"](#).

Étapes

1. Sélectionnez **ILM > Storage pools**.

L'onglet Pools de stockage répertorie tous les pools de stockage définis.



Pour les nouvelles installations de StorageGRID 11.6 ou version antérieure, le pool de stockage « All Storage Nodes » est automatiquement mis à jour lorsque vous ajoutez de nouveaux sites de centre de données. N'utilisez pas ce pool dans les règles ILM.

2. Pour créer un nouveau pool de stockage, sélectionnez **Créer**.
3. Saisissez un nom unique pour le pool de stockage. Utilisez un nom facile à identifier lors de la configuration des profils de codage d'effacement et des règles ILM.
4. Dans la liste déroulante **Site**, sélectionnez un site pour ce pool de stockage.

Lorsque vous sélectionnez un site, le nombre de nœuds de stockage dans le tableau est automatiquement mis à jour.

En règle générale, n'utilisez pas le site « All Sites » dans un pool de stockage. Les règles ILM qui utilisent un pool de stockage « All Sites » placent les objets sur n'importe quel site disponible, ce qui vous donne moins de contrôle sur le placement des objets. De plus, un pool de stockage « All Sites » utilise immédiatement les Storage Nodes d'un nouveau site, ce qui pourrait ne pas être le comportement que vous attendez.

5. Dans la liste déroulante **Niveau de stockage**, sélectionnez le type de stockage qui sera utilisé si une règle ILM utilise ce pool de stockage.

Le niveau de stockage, *incluant tous les niveaux de stockage*, comprend tous les nœuds de stockage du site sélectionné. Si vous avez créé des niveaux de stockage supplémentaires pour les nœuds de stockage de votre grille, ils sont répertoriés dans la liste déroulante.

6. Si vous souhaitez utiliser le pool de stockage dans un profil de codage d'effacement multisite, sélectionnez **Ajouter plus de nœuds** pour ajouter une entrée pour chaque site au pool de stockage.



Vous recevez un avertissement si vous ajoutez plusieurs entrées avec des niveaux de stockage différents pour un site.

Pour supprimer une entrée, sélectionnez l'icône de suppression **X**.

7. Lorsque vous êtes satisfait de vos sélections, sélectionnez **Enregistrer**.

Le nouveau pool de stockage est ajouté à la liste.

Afficher les détails du pool de stockage dans StorageGRID

Vous pouvez consulter les détails d'un pool de stockage pour déterminer où le pool de stockage est utilisé et pour voir quels nœuds et niveaux de stockage sont inclus.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **ILM > Storage pools**.

Le tableau des pools de stockage comprend les informations suivantes pour chaque pool de stockage contenant des nœuds de stockage :

- **Nom** : Le nom d'affichage unique du pool de stockage.
- **Nombre de nœuds** : Le nombre de nœuds dans le pool de stockage.
- **Utilisation du stockage** : Pourcentage de l'espace utilisable total utilisé pour les données d'objet sur ce nœud. Cette valeur n'inclut pas les métadonnées des objets.
- **Capacité totale** : La taille du pool de stockage, qui correspond à la quantité totale d'espace utilisable pour les données d'objets pour tous les nœuds du pool de stockage.
- **Utilisation ILM** : Comment le pool de stockage est actuellement utilisé. Un pool de stockage peut être inutilisé ou utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.

2. Pour afficher les détails d'un pool de stockage spécifique, sélectionnez son nom.

La page de détails du pool de stockage s'affiche.

3. Consultez l'onglet **Nœuds** pour en savoir plus sur les nœuds de stockage inclus dans le pool de stockage.

Le tableau comprend les informations suivantes pour chaque nœud :

- Nom du nœud
- Nom du site
- Niveau de stockage
- Utilisation du stockage : le pourcentage de l'espace total utilisable pour les données d'objet qui a été utilisé pour le nœud de stockage.



La même valeur d'utilisation du stockage (%) est également affichée dans le graphique Stockage utilisé - Données d'objet pour chaque nœud de stockage (sélectionnez **Nœuds > Nœud de stockage > Stockage**).

4. Consultez l'onglet **Utilisation ILM** pour déterminer si le pool de stockage est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
5. Vous pouvez également accéder à la page **règles ILM** pour en savoir plus sur les règles qui utilisent le pool de stockage et les gérer.

Voir la ["instructions pour travailler avec les règles ILM"](#).

Modifier un pool de stockage dans StorageGRID

Vous pouvez modifier un pool de stockage pour changer son nom ou pour mettre à jour les sites et les niveaux de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez examiné le ["directives pour la création de pools de stockage"](#).
- \${post_edited_translations.segment}

À propos de cette tâche

Si vous ajoutez un nouveau site ou un nouveau niveau de stockage à un pool de stockage utilisé dans la stratégie ILM active, sachez que les nœuds de stockage du nouveau site ou du nouveau niveau de stockage ne seront pas utilisés automatiquement. Pour forcer StorageGRID à utiliser un nouveau site ou un nouveau niveau de stockage, vous devez activer une nouvelle stratégie ILM après avoir enregistré le pool de stockage modifié.

Étapes

1. Sélectionnez **ILM > Storage pools**.
2. Cochez la case correspondant au pool de stockage que vous souhaitez modifier.

\${post_edited_translations.segment}

3. Sélectionnez **Modifier**.

4. `${post_edited_translations.segment}`
5. Au besoin, sélectionnez d'autres sites et niveaux de stockage.

Vous ne pouvez pas modifier le site ou le niveau de stockage si le pool de stockage est utilisé dans un profil de code d'effacement et que cette modification rendrait le schéma de code d'effacement non valide. Par exemple, si un pool de stockage utilisé dans un profil de code d'effacement comprend actuellement un niveau de stockage avec un seul site, vous ne pouvez pas utiliser un niveau de stockage avec deux sites car cette modification rendrait le schéma de code d'effacement non valide.



L'ajout ou la suppression de sites d'un pool de stockage existant ne déplacera pas les données codées par effacement existantes. Si vous souhaitez déplacer les données existantes du site, vous devez créer un nouveau pool de stockage et un nouveau profil EC pour réencoder les données.

6. Sélectionnez **Enregistrer**.

Après avoir terminé

Si vous avez ajouté un nouveau site ou une nouvelle classe de stockage à un pool de stockage utilisé dans la politique ILM active, activez une nouvelle politique ILM pour forcer StorageGRID à utiliser le nouveau site ou la nouvelle classe de stockage. Par exemple, clonez votre politique ILM existante, puis activez le clone. Voir `"${post_edited_translations.segment}"`.

Supprimer un pool de stockage dans StorageGRID

Vous pouvez supprimer un pool de stockage qui n'est pas utilisé.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Étapes

1. Sélectionnez **ILM > Storage pools**.
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 codage d'effacement. Le cas échéant, sélectionnez **storage pool name > ILM usage** pour déterminer où le pool de stockage est utilisé.

3. Si le pool de stockage que vous souhaitez supprimer n'est pas utilisé, cochez la case.
4. Sélectionnez **Remove**.
5. Sélectionnez **OK**.

`${post_edited_translations.segment}`

Découvrez les Cloud Storage Pools dans StorageGRID

Un pool de stockage cloud vous permet d'utiliser ILM pour déplacer les données d'objets en dehors de votre système StorageGRID. Par exemple, vous pouvez déplacer des objets rarement consultés vers un stockage cloud à moindre coût, comme Amazon S3

Glacier, S3 Glacier Deep Archive, Google Cloud ou le niveau d'accès Archive dans Microsoft Azure Blob storage. Ou, vous pouvez conserver une sauvegarde cloud des objets StorageGRID pour améliorer la reprise après sinistre.

Du point de vue de l'ILM, un pool de stockage cloud est similaire à un pool de stockage. Pour stocker des objets à l'un ou l'autre emplacement, vous sélectionnez le pool lors de la création des instructions de placement d'une règle ILM. Cependant, alors que les pools de stockage sont constitués de nœuds de stockage au sein du système StorageGRID, un pool de stockage cloud est constitué d'un compartiment externe (S3) ou d'un conteneur (Azure Blob storage).

Le tableau compare les pools de stockage aux Cloud Storage Pools et présente les principales similitudes et différences.

	Pool de stockage	Pool de stockage cloud
Comment est-il créé ?	Utilisation de l'option ILM > Storage pools dans Grid Manager.	Utiliser l'option ILM > Pools de stockage > Cloud Storage Pools dans Grid Manager. Vous devez configurer le bucket ou le conteneur externe avant de pouvoir créer le Cloud Storage Pool.
Combien de pools pouvez-vous créer ?	Illimité.	Jusqu'à 10.
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage au sein de StorageGRID.	Dans un compartiment Amazon S3, un conteneur de stockage Azure Blob ou un Google Cloud externe au système StorageGRID. Si le pool de stockage cloud est un compartiment Amazon S3 : • Vous pouvez, si vous le souhaitez, configurer un cycle de vie de compartiment pour transférer les objets vers un stockage à long terme à faible coût, tel qu'Amazon S3 Glacier ou S3 Glacier Deep Archive. Le système de stockage externe doit prendre en charge la classe de stockage Glacier et l'API S3 RestoreObject. • Vous pouvez créer des pools de stockage cloud à utiliser avec AWS Commercial Cloud Services (C2S), qui prend en charge la AWS Secret Region. Si le pool de stockage cloud est un conteneur de stockage Blob Azure, StorageGRID transfère l'objet vers le niveau Archive. Remarque : En général, ne configurez pas la gestion du cycle de vie du stockage Blob Azure pour le conteneur utilisé pour un Cloud Storage Pool. RestoreObject opérations sur les objets dans le Cloud Storage Pool peuvent être affectées par le cycle de vie configuré.

	Pool de stockage	Pool de stockage cloud
Qu'est-ce qui contrôle le placement des objets ?	Une règle ILM dans les politiques ILM actives.	Une règle ILM dans les politiques ILM actives.
Quelle méthode de protection des données est utilisée ?	Réplication ou code d'effacement.	Réplication.
Combien de copies de chaque objet sont autorisées ?	Plusieurs.	Une copie dans le Cloud Storage Pool et, éventuellement, une ou plusieurs copies dans StorageGRID. Remarque : Vous ne pouvez pas stocker un objet dans plus d'un Cloud Storage Pool à la fois.
Quels sont les avantages ?	Les objets sont rapidement accessibles à tout moment.	Stockage à faible coût. Remarque : les données FabricPool ne peuvent pas être hiérarchisées vers des Cloud Storage Pools.

Cycle de vie d'un objet Cloud Storage Pool dans StorageGRID

Avant de mettre en œuvre des Cloud Storage Pools, examinez le cycle de vie des objets stockés dans chaque type de Cloud Storage Pool.

S3 : Cycle de vie d'un objet de Cloud Storage Pool

`${post_edited_translations.segment}`



Le terme « 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 Expedited. Seuls les modes de récupération Bulk ou Standard sont pris en charge.



La plateforme Google Cloud (GCP) prend en charge la récupération d'objets à partir d'un stockage à long terme sans nécessiter d'opération POST Restore.

1. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

2. `${post_edited_translations.segment}`

- Lorsque l'objet correspond à une règle ILM qui utilise un S3 Cloud Storage Pool comme emplacement de placement, StorageGRID déplace l'objet vers le compartiment S3 externe spécifié par le Cloud Storage Pool.

- Lorsque l'objet a été déplacé vers le pool de stockage cloud S3, l'application cliente peut le récupérer à l'aide d'une requête S3 GetObject depuis StorageGRID, sauf si l'objet a été transféré vers le stockage Glacier.

3. Objet transféré vers Glacier (état non récupérable)

- L'objet peut éventuellement être transféré vers le stockage Glacier. Par exemple, le compartiment S3 externe peut utiliser une configuration de cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après un certain nombre de jours.



Si vous souhaitez effectuer une transition d'objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API S3 RestoreObject.

- Durant la transition, l'application cliente peut utiliser une requête S3 HeadObject pour surveiller l'état de l'objet.

4. \${post_edited_translations.segment}

Si un objet a été transféré vers le stockage Glacier, l'application cliente peut émettre une requête S3 RestoreObject pour restaurer une copie récupérable dans le pool de stockage cloud S3. La requête précise combien de jours la copie doit être disponible dans le pool de stockage cloud et le niveau d'accès aux données à utiliser pour l'opération de restauration (Expedited, Standard ou Bulk). Lorsque la date d'expiration de la copie récupérable est atteinte, la copie redevient automatiquement non récupérable.



Si une ou plusieurs copies de l'objet existent également sur des nœuds de stockage au sein de StorageGRID, il n'est pas nécessaire de restaurer l'objet depuis Glacier en émettant une requête RestoreObject. À la place, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

5. Objet récupéré

Une fois l'objet restauré, l'application cliente peut envoyer une requête GetObject pour récupérer l'objet restauré.

Azure : Cycle de vie d'un objet de pool de stockage cloud

\${post_edited_translations.segment}

1. \${post_edited_translations.segment}

\${post_edited_translations.segment}

2. \${post_edited_translations.segment}

Lorsque l'objet correspond à une règle ILM qui utilise un Azure Cloud Storage Pool comme emplacement de placement, StorageGRID déplace l'objet vers le conteneur Azure Blob storage externe spécifié par le Cloud Storage Pool.

3. \${post_edited_translations.segment}

\${post_edited_translations.segment}

4. Objet restauré à partir du niveau Archive

Si un objet a été transféré vers le niveau Archive, l'application cliente peut émettre une requête S3 RestoreObject pour restaurer une copie récupérable dans le pool de stockage Azure Cloud Storage.

Lorsque StorageGRID reçoit le RestoreObject, il fait passer temporairement l'objet vers le niveau Cool du stockage Azure Blob. Dès que la date d'expiration de la demande RestoreObject est atteinte, StorageGRID fait repasser l'objet vers le niveau Archive.



Si une ou plusieurs copies de l'objet existent également sur des nœuds de stockage au sein de StorageGRID, il n'est pas nécessaire de restaurer l'objet depuis le niveau d'accès Archive en émettant une requête RestoreObject. À la place, vous pouvez récupérer directement la copie locale à l'aide d'une requête GetObject.

5. Objet récupéré

Une fois qu'un objet a été restauré dans le pool de stockage cloud Azure, l'application cliente peut émettre une requête GetObject pour récupérer l'objet restauré.

Informations connexes

["Utilisez l'API REST S3"](#)

Cas d'utilisation des Cloud Storage Pool dans StorageGRID

Avec les Cloud Storage Pools, vous pouvez sauvegarder ou hiérarchiser des données vers un emplacement externe. De plus, vous pouvez sauvegarder ou hiérarchiser des données vers plusieurs clouds.

Sauvegardez les données StorageGRID sur un emplacement externe.

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder les objets StorageGRID sur un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, les données d'objet dans le pool de stockage cloud peuvent être utilisées pour répondre aux requêtes des clients. Toutefois, vous devrez peut-être émettre une requête S3 RestoreObject pour accéder à la copie d'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objets présentes dans un Cloud Storage Pool peuvent également servir à récupérer des données perdues sur StorageGRID suite à une panne de volume de stockage ou de nœud de stockage. Si la seule copie restante d'un objet se trouve dans un Cloud Storage Pool, StorageGRID restaure temporairement l'objet et en crée une nouvelle copie sur le nœud de stockage récupéré.

`${post_edited_translations.segment}`

1. Créez un seul pool de stockage cloud.
2. Configurez une règle ILM qui stocke simultanément des copies d'objets sur des Storage Nodes (sous forme de copies répliquées ou codées par effacement) et une seule copie d'objet dans le Cloud Storage Pool.
3. Ajoutez la règle à votre politique ILM. Ensuite, simulez et activez la politique.

Transférez les données de niveau de StorageGRID vers un emplacement externe

Vous pouvez utiliser un Cloud Storage Pool pour stocker des objets en dehors du système StorageGRID. Par exemple, supposons que vous ayez un grand nombre d'objets à conserver, mais que vous prévoyiez d'y

accéder rarement, voire jamais. Vous pouvez utiliser un Cloud Storage Pool pour hiérarchiser les objets vers un stockage moins coûteux et libérer de l'espace dans StorageGRID.

Pour mettre en œuvre une solution de hiérarchisation :

1. Créez un seul pool de stockage cloud.
2. Configurez une règle ILM qui déplace les objets rarement utilisés des nœuds de stockage vers le Cloud Storage Pool.
3. Ajoutez la règle à votre politique ILM. Ensuite, simulez et activez la politique.

`${post_edited_translations.segment}`

Vous pouvez configurer plusieurs points de terminaison Cloud Storage Pool si vous souhaitez hiérarchiser ou sauvegarder des données d'objet vers plus d'un cloud. Les filtres de vos règles ILM vous permettent de spécifier quels objets sont stockés dans chaque Cloud Storage Pool. Par exemple, vous pouvez stocker des objets de certains locataires ou compartiments dans Amazon S3 Glacier et des objets d'autres locataires ou compartiments dans Azure Blob storage. Ou vous pouvez déplacer des données entre Amazon S3 Glacier et Azure Blob storage.



`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

1. Créez jusqu'à 10 Cloud Storage Pools.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment opportun dans chaque Cloud Storage Pool. Par exemple, stockez les objets du bucket A dans Cloud Storage Pool A, et stockez les objets du bucket B dans Cloud Storage Pool B. Ou, stockez les objets dans Cloud Storage Pool A pendant une certaine période, puis déplacez-les vers Cloud Storage Pool B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simulez et activez la politique.

Exigences et limites des Cloud Storage Pool dans StorageGRID

Si vous prévoyez d'utiliser un Cloud Storage Pool pour déplacer des objets hors du système StorageGRID, vous devez examiner les considérations relatives à la configuration et à l'utilisation des Cloud Storage Pools.

Considérations générales

- En général, le stockage d'archives cloud, tel que Amazon S3 Glacier ou Azure Blob storage, est un endroit peu coûteux pour stocker des données d'objets. Cependant, les coûts pour récupérer des données depuis le stockage d'archives cloud sont relativement élevés. Pour obtenir le coût global le plus bas, vous devez prendre en compte quand et à quelle fréquence vous accéderez aux objets dans le Cloud Storage Pool. L'utilisation d'un Cloud Storage Pool est recommandée uniquement pour le contenu auquel vous prévoyez d'accéder rarement.
- L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence supplémentaire nécessaire pour récupérer un objet depuis la cible du pool de stockage cloud.
- Les objets avec le verrouillage d'objet S3 activé ne peuvent pas être placés dans des Cloud Storage Pools.
- Les combinaisons suivantes de plateforme, d'authentification et de protocole avec S3 Object lock ne sont pas prises en charge pour les Cloud Storage Pools :

- **Plateformes** : Google Cloud Platform et Azure
- **Types d'authentification** : Accès anonyme
- **Protocole** : HTTP

Considérations relatives aux ports utilisés pour les pools de stockage cloud

Pour que les règles ILM puissent déplacer des objets vers et depuis le Cloud Storage Pool spécifié, vous devez configurer le ou les réseaux contenant les Storage Nodes de votre système. Vous devez vous assurer que les ports suivants peuvent communiquer avec le Cloud Storage Pool.

Par défaut, les pools de stockage cloud utilisent les ports suivants :

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

Vous pouvez spécifier un port différent lors de la création ou de la modification d'un Cloud Storage Pool.

Si vous utilisez un serveur proxy non transparent, vous devez également "[configurer un proxy de stockage](#)" autoriser 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 Cloud Storage Pool nécessite une connectivité réseau au cloud. Vous devez prendre en compte le coût de l'infrastructure réseau que vous utiliserez pour accéder au cloud et la dimensionner de manière appropriée, en fonction de la quantité de données que vous prévoyez de transférer entre StorageGRID et le cloud à l'aide du Cloud Storage Pool.

Lorsque StorageGRID se connecte au point de terminaison du Cloud Storage Pool externe, il émet diverses requêtes pour surveiller la connectivité et s'assurer qu'il peut effectuer les opérations requises. Bien que ces requêtes engendrent des coûts supplémentaires, le coût de la surveillance d'un Cloud Storage Pool ne devrait représenter qu'une faible fraction du coût total du stockage d'objets dans S3 ou Azure.

Des coûts plus importants peuvent s'appliquer si vous devez déplacer des objets d'un point de terminaison de Cloud Storage Pool externe vers StorageGRID. Les objets peuvent être déplacés vers StorageGRID dans l'un ou l'autre des cas suivants :

- L'unique copie de l'objet se trouve dans un Cloud Storage Pool et vous décidez de stocker l'objet dans StorageGRID à la place. Dans ce cas, vous reconfigurez vos règles et votre politique ILM. Lors de l'évaluation ILM, StorageGRID effectue plusieurs requêtes pour récupérer l'objet depuis le Cloud Storage Pool. StorageGRID crée ensuite localement le nombre spécifié de copies répliquées ou à codage d'effacement. Après que l'objet a été déplacé vers StorageGRID, la copie dans le Cloud Storage Pool est supprimée.
- Des objets sont perdus suite à une panne d'un nœud de stockage. Si la seule copie restante d'un objet se trouve dans un Cloud Storage Pool, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage récupéré.



Lorsque des objets sont déplacés vers StorageGRID depuis un pool de stockage cloud, StorageGRID envoie plusieurs requêtes au point de terminaison du pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, veuillez contacter le support technique pour obtenir une estimation du délai et des coûts associés.

S3 : Autorisations requises pour le compartiment Cloud Storage Pool

Les politiques du compartiment S3 externe utilisé pour un Cloud Storage Pool doivent accorder à StorageGRID l'autorisation de déplacer un objet vers le compartiment, de consulter le statut d'un objet, de restaurer un objet depuis le stockage Glacier si nécessaire, et plus encore. Idéalement, StorageGRID devrait disposer d'un accès complet au compartiment(s3 : * ; cependant, si cela n'est pas possible, la politique du 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 relatives au cycle de vie du compartiment externe

Le déplacement d'objets entre StorageGRID et le compartiment S3 externe spécifié dans le Cloud Storage Pool est contrôlé par les règles ILM et les politiques ILM actives dans StorageGRID. En revanche, la transition des objets du compartiment S3 externe spécifié dans le Cloud Storage Pool 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 transférer des objets depuis le Cloud Storage Pool, vous devez créer la configuration de cycle de vie appropriée sur le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API S3 RestoreObject.

Par exemple, supposons que vous souhaitiez que tous les objets déplacés de StorageGRID vers le Cloud Storage Pool soient immédiatement transférés vers le stockage Amazon S3 Glacier. Vous créeriez alors une configuration de cycle de vie sur le compartiment S3 externe spécifiant une action unique (**Transition**) comme suit :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Cette règle transférerait tous les objets du compartiment vers Amazon S3 Glacier le jour de leur création (c'est-à-dire le jour où ils ont été déplacés de StorageGRID vers le Cloud Storage Pool).



Lors de la configuration du cycle de vie du compartiment externe, n'utilisez jamais les actions **Expiration** pour définir la date d'expiration des objets. Les actions d'expiration entraînent la suppression des objets expirés par le système de stockage externe. Si vous tentez ultérieurement d'accéder à un objet expiré depuis StorageGRID, l'objet supprimé sera introuvable.

Si vous souhaitez transférer des objets du Cloud Storage Pool vers S3 Glacier Deep Archive (au lieu d'Amazon S3 Glacier), spécifiez `<StorageClass>DEEP_ARCHIVE</StorageClass>` dans le cycle de vie du compartiment. Cependant, notez que vous ne pouvez pas utiliser le niveau `Expedited` pour restaurer des objets depuis S3 Glacier Deep Archive.

Azure : Considérations relatives au niveau d'accès

Lors de la configuration d'un compte de stockage Azure, vous pouvez définir le niveau d'accès par défaut sur Hot ou Cool. Lors de la création d'un compte de stockage destiné à être utilisé avec un Cloud Storage Pool, vous devez utiliser le niveau Hot comme niveau par défaut. Même si StorageGRID définit immédiatement le niveau sur Archive lorsqu'il déplace des objets vers le Cloud Storage Pool, l'utilisation du niveau Hot par défaut garantit que vous ne serez pas facturé de frais de suppression anticipée pour les objets retirés du niveau Cool avant la période minimale de 30 jours.

Azure : la gestion du cycle de vie n'est pas prise en charge

N'utilisez pas la gestion du cycle de vie du stockage Blob Azure pour le conteneur utilisé avec un Cloud Storage Pool. Les opérations de cycle de vie pourraient interférer avec les opérations du Cloud Storage Pool.

Informations connexes

["Créer un pool de stockage cloud"](#)

Pools de stockage cloud et réplication CloudMirror dans StorageGRID

Lorsque vous commencerez à utiliser Cloud Storage Pools, il peut être utile de comprendre les similitudes et les différences entre Cloud Storage Pools et le service de réplication CloudMirror de StorageGRID.

	Pool de stockage cloud	CloudMirror service de réplication
Quel est l'objectif principal ?	Sert de cible d'archivage. La copie de l'objet dans le Cloud Storage Pool peut être la seule copie de l'objet, ou une copie supplémentaire. Autrement dit, au lieu de conserver deux copies sur site, vous pouvez en conserver une dans StorageGRID et envoyer une copie vers le Cloud Storage Pool.	Permet à un locataire de répliquer automatiquement des objets d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). Crée une copie indépendante d'un objet dans une infrastructure S3 indépendante.

	Pool de stockage cloud	CloudMirror service de réplication
Comment est-ce configuré ?	Définis de la même manière que les pools de stockage, à l'aide du Grid Manager ou de l'API de gestion de la grille. Peuvent être sélectionnés comme emplacement de placement dans une règle ILM. Alors qu'un pool de stockage est constitué d'un groupe de Storage Nodes, un Cloud Storage Pool est défini à l'aide d'un point de terminaison S3 ou Azure distant (adresse IP, informations d'identification, etc.).	Un utilisateur locataire " configure la réplication CloudMirror " peut définir un point de terminaison CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire de locataires ou de l'API S3. Une fois le point de terminaison CloudMirror configuré, tout compartiment appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.
Qui est responsable de sa mise en place ?	En général, un administrateur de grille	En règle générale, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Niveau d'archivage Azure Blob • Google Cloud Platform (GCP)	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Une ou plusieurs règles ILM dans les politiques ILM actives. Les règles ILM définissent quels objets StorageGRID déplace vers le Cloud Storage Pool et quand les objets sont déplacés.	L'action d'ingérer un nouvel objet dans un compartiment source qui a été configuré avec un point de terminaison CloudMirror. Les objets qui existaient dans le compartiment source avant que celui-ci ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.
Comment les objets sont-ils récupérés ?	Les applications doivent adresser des requêtes à StorageGRID pour récupérer les objets déplacés vers un Cloud Storage Pool. Si l'unique copie d'un objet a été transférée vers un stockage d'archivage, StorageGRID gère le processus de restauration de l'objet afin qu'il puisse être récupéré.	Comme la copie miroir dans le compartiment de destination est une copie indépendante, les applications peuvent récupérer l'objet en effectuant des requêtes soit auprès de StorageGRID, soit auprès de la destination S3. Par exemple, supposons que vous utilisiez la réplication CloudMirror pour dupliquer des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.

	Pool de stockage cloud	CloudMirror service de réplication
Pouvez-vous lire directement depuis la destination ?	Non. Les objets déplacés vers un pool de stockage cloud sont gérés par StorageGRID. Les requêtes de lecture doivent être adressées à StorageGRID (et StorageGRID sera responsable de la récupération depuis le pool de stockage cloud).	Oui, car la copie miroir est une copie indépendante.
Que se passe-t-il si un objet est supprimé de la source ?	L'objet est également supprimé du Cloud Storage Pool.	La 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 une catastrophe (StorageGRID system non opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Durant ce processus, des copies d'objets répliqués peuvent être restaurées à partir des copies présentes dans le Cloud Storage Pool.	Les copies d'objets dans la destination CloudMirror sont indépendantes de StorageGRID, elles peuvent donc être consultées directement avant que les nœuds StorageGRID ne soient récupérés.

Créez un Cloud Storage Pool dans StorageGRID

Un pool de stockage cloud spécifie un seul compartiment Amazon S3 externe, un autre fournisseur compatible S3 ou un conteneur de stockage Azure Blob.

Lorsque vous créez un pool de stockage cloud, vous spécifiez le nom et l'emplacement du compartiment ou du conteneur externe que StorageGRID utilisera pour stocker les objets, le type de fournisseur de cloud (Amazon S3/GCP ou Azure Blob storage), ainsi que les informations dont StorageGRID a besoin pour accéder au compartiment ou au conteneur externe.

StorageGRID valide le Cloud Storage Pool dès que vous l'enregistrez, vous devez donc vous assurer que le bucket ou le conteneur spécifié dans le Cloud Storage Pool existe et est accessible.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).
- Vous avez examiné le ["considérations relatives aux pools de stockage cloud"](#).
- Le compartiment ou conteneur externe référencé par le pool de stockage cloud existe déjà, et vous disposez du [Informations sur le point de terminaison du service](#).
- Pour accéder au seau ou au conteneur, vous avez le [informations de compte pour le type d'authentification](#) que vous choisirez.

Étapes

1. Sélectionnez **ILM > Pools de stockage > Cloud Storage Pools**.
2. Sélectionnez **Créer**, puis saisissez les informations suivantes :

Champ	Description
Nom du pool de stockage cloud	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Utilisez un nom qui sera facile à identifier lorsque vous configurerez les règles ILM.
Type de fournisseur	Quel fournisseur de cloud allez-vous utiliser pour ce Cloud Storage Pool ? • Amazon S3/GCP : Sélectionnez cette option pour un fournisseur Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou autre fournisseur compatible S3. • Stockage Blob Azure
Bucket ou conteneur	Nom du compartiment S3 externe ou du conteneur Azure. Vous ne pouvez pas modifier cette valeur après l'enregistrement du Cloud Storage Pool.

3. En fonction de votre sélection de type de fournisseur, saisissez les informations du point de terminaison de service.

Amazon S3/GCP

- a. Pour le protocole, sélectionnez soit HTTPS, soit HTTP.



N'utilisez pas de connexions HTTP pour les données sensibles.

- b. Saisissez le nom d'hôte. Exemple :

`s3-aws-region.amazonaws.com`

- c. Sélectionnez le style d'URL :

Option	Description
Détection automatique	Le système tentera de détecter automatiquement le style d'URL à utiliser, en fonction des informations fournies. Par exemple, si vous indiquez une adresse IP, StorageGRID utilisera une URL de type chemin. Sélectionnez cette option uniquement si vous ne savez pas quel style spécifique utiliser.
style hébergé virtuellement	Utilisez une URL de type hébergement virtuel pour accéder au compartiment. Les URL de type hébergement virtuel incluent le nom du compartiment dans le nom de domaine. Exemple : <code>https://bucket-name.s3.company.com/key-name</code>
Style de chemin	Utilisez une URL de type chemin pour accéder au compartiment. Les URL de type chemin incluent le nom du compartiment à la fin. Exemple : <code>https://s3.company.com/bucket-name/key-name</code> Remarque : L'option d'URL de type chemin n'est pas recommandée et sera obsolète dans une future version de StorageGRID.

- d. Vous pouvez également saisir le numéro de port, ou utiliser le port par défaut : 443 pour HTTPS ou 80 pour HTTP.

Stockage Blob Azure

- a. En utilisant l'un des formats suivants, saisissez l'URI du point de terminaison du service.

- `https://host:port`
- `http://host:port`

Exemple : `https://myaccount.blob.core.windows.net:443`

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour HTTPS et le port 80 est utilisé pour HTTP.

4. Sélectionnez **Continuer**. Sélectionnez ensuite le type d'authentification et saisissez les informations requises pour le point de terminaison Cloud Storage Pool :

Clé d'accès

Pour Amazon S3/GCP ou tout autre fournisseur compatible S3

- a. **ID de clé d'accès** : Saisissez l'ID de clé d'accès du compte propriétaire du compartiment externe.
- b. **Clé d'accès secrète** : Saisissez la clé d'accès secrète.

IAM Roles Anywhere

Pour le service AWS IAM Roles Anywhere

StorageGRID utilise le service AWS Security Token Service (STS) pour générer dynamiquement un jeton à courte durée de vie afin d'accéder aux ressources AWS.

- a. **Région AWS IAM Roles Anywhere** : sélectionnez la région du pool de stockage cloud. Par exemple, `us-east-1`.
- b. **URN de l'ancre de confiance** : Saisissez l'URN de l'ancre de confiance qui valide les demandes d'informations d'identification STS éphémères. Peut être une autorité de certification racine ou intermédiaire.
- c. **URN du profil** : Saisissez l'URN du profil IAM Roles Anywhere qui répertorie les rôles pouvant être assumés par toute personne de confiance.
- d. **URN du rôle** : Saisissez l'URN du rôle IAM qui peut être assumé par toute personne de confiance.
- e. **Durée de la session** : Indiquez la durée des informations d'identification de sécurité temporaires et de la session de rôle. Saisissez au moins 15 minutes et au plus 12 heures.
- f. **Certificat d'autorité de certification du serveur** (facultatif) : Un ou plusieurs certificats d'autorité de certification de confiance, au format PEM, pour vérifier le serveur IAM Roles Anywhere. Si ce certificat est omis, le serveur ne sera pas vérifié.
- g. **Certificat d'entité finale** : la clé publique, au format PEM, du certificat X509 signé par le trust anchor. AWS IAM Roles Anywhere utilise cette clé pour émettre un jeton STS.
- h. **Clé privée de l'entité finale** : la clé privée du certificat de l'entité finale.

CAP (portail d'accès C2S)

Pour le service S3 Commercial Cloud Services (C2S)

- a. **URL des informations d'identification temporaires** : Saisissez l'URL complète que StorageGRID utilisera pour obtenir des informations d'identification temporaires auprès du serveur CAP, y compris tous les paramètres API requis et facultatifs attribués à votre compte C2S.
- b. **Certificat d'autorité de certification du serveur** : Sélectionnez **Parcourir** et téléchargez le certificat d'autorité de certification que StorageGRID utilisera pour vérifier le serveur CAP. Le certificat doit être au format PEM et délivré par une autorité de certification gouvernementale compétente (CA).
- c. **Certificat client** : Sélectionnez **Parcourir** et téléchargez le certificat que StorageGRID utilisera pour s'identifier auprès du serveur CAP. Le certificat client doit être au format PEM, émis par une autorité de certification gouvernementale compétente et disposer des droits d'accès à votre compte C2S.
- d. **Clé privée du client** : Sélectionnez **Parcourir** et téléchargez la clé privée encodée au format PEM pour le certificat client.

- e. Si la clé privée du client est chiffrée, saisissez la phrase secrète permettant de déchiffrer la clé privée du client. Sinon, laissez le champ **Phrase secrète de la clé privée du client** vide.



Si le certificat client doit être chiffré, utilisez le format traditionnel pour le chiffrement. Le format de chiffrement PKCS #8 n'est pas pris en charge.

Stockage Blob Azure

Pour Azure Blob Storage, clé partagée uniquement

- a. **Nom du compte** : Saisissez le nom du compte de stockage qui possède le conteneur externe
b. **Clé de compte** : Saisissez la clé secrète du compte de stockage

Vous pouvez utiliser le portail Azure pour trouver ces valeurs.

Anonyme

Aucune information supplémentaire n'est requise.

5. Sélectionnez **Continuer**. Choisissez ensuite le type de vérification du serveur que vous souhaitez utiliser :

Option	Description
Utilisez les certificats d'autorité de certification racine dans le système d'exploitation du nœud de stockage	Utilisez les certificats d'autorité de certification Grid installés sur le système d'exploitation pour sécuriser les connexions.
Utilisez un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. Sélectionnez Parcourir et téléchargez le certificat au format PEM.
Ne pas vérifier le certificat	Sélectionner cette option signifie que les connexions TLS au Cloud Storage Pool ne sont pas sécurisées.

6. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide que le compartiment ou le conteneur et le point de terminaison du service existent et qu'ils sont accessibles à l'aide des informations d'identification que vous avez spécifiées.
- Crée un fichier marqueur dans le compartiment ou le conteneur pour l'identifier comme un Cloud Storage Pool. Ne supprimez jamais ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

En cas d'échec de la validation du Cloud Storage Pool, un message d'erreur expliquant la raison de cet échec s'affiche. Par exemple, une erreur peut être signalée en cas de problème de certificat ou si le bucket ou le container que vous avez spécifié n'existe pas déjà.

7. En cas d'erreur, consultez la "[Instructions de dépannage des Cloud Storage Pools](#)", résolvez les problèmes éventuels, puis essayez à nouveau d'enregistrer le Cloud Storage Pool.

Afficher les détails du pool de stockage cloud dans StorageGRID

Vous pouvez consulter les détails d'un Cloud Storage Pool pour déterminer où il est utilisé et voir quels nœuds et niveaux de stockage sont inclus.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **ILM > Pools de stockage > Cloud Storage Pools**.

Le tableau des pools de stockage cloud comprend les informations suivantes pour chaque pool de stockage cloud contenant des nœuds de stockage :

- **Nom** : Le nom d'affichage unique du pool.
- **URI** : L'identifiant uniforme de ressource (Uniform Resource Identifier) du pool de stockage cloud.
- **Type de fournisseur** : Quel fournisseur de cloud est utilisé pour ce Cloud Storage Pool.
- **Conteneur** : le nom du compartiment utilisé pour le Cloud Storage Pool.
- **Utilisation ILM** : Comment le pool est actuellement utilisé. Un pool de stockage cloud peut être inutilisé ou utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.
- **Dernière erreur** : La dernière erreur détectée lors d'une vérification de l'état de ce Cloud Storage Pool.

2. Pour afficher les détails d'un pool de stockage cloud spécifique, sélectionnez son nom.

La page de détails du pool s'affiche.

3. Consultez l'onglet **Authentification** pour en savoir plus sur le type d'authentification de ce Cloud Storage Pool et pour modifier les détails d'authentification.
4. Consultez l'onglet **Vérification du serveur** pour en savoir plus sur les détails de la vérification, modifier la vérification, télécharger un nouveau certificat ou copier le PEM du certificat.
5. Consultez l'onglet **Utilisation ILM** pour déterminer si le Cloud Storage Pool est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
6. Vous pouvez également vous rendre sur la page des règles ILM pour ["Découvrez et gérez toutes les règles"](#) qui utilisent le pool de stockage cloud.

Modifier un Cloud Storage Pool dans StorageGRID

Vous pouvez modifier un pool de stockage cloud pour en changer le nom, le point de terminaison de service ou d'autres détails ; toutefois, vous ne pouvez pas changer le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez examiné le ["considérations relatives aux pools de stockage cloud"](#).

Étapes

1. Sélectionnez **ILM > Pools de stockage > Cloud Storage Pools**.

Le tableau « Pools de stockage cloud » répertorie les pools de stockage cloud existants.

2. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

3. Si nécessaire, modifiez le nom du Cloud Storage Pool, le point de terminaison du service, les paramètres d'authentification ou la méthode de vérification du certificat.



Vous ne pouvez pas modifier le type de fournisseur, le compartiment S3 ou le conteneur Azure pour un Cloud Storage Pool.

`${post_edited_translations.segment}`

4. Sélectionnez **Enregistrer**.

`${post_edited_translations.segment}`

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.

Consultez les instructions concernant "`${post_edited_translations.segment}`", résolvez le problème, puis essayez d'enregistrer à nouveau le Cloud Storage Pool.

Supprimer un Cloud Storage Pool dans StorageGRID

Vous pouvez supprimer un pool de stockage cloud s'il n'est pas utilisé dans une règle ILM et s'il ne contient pas de données d'objet.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[autorisations d'accès requises](#)".

Si nécessaire, utilisez ILM pour déplacer les données d'objet

Si le Cloud Storage Pool que vous souhaitez supprimer contient des données d'objet, vous devez utiliser ILM pour déplacer les données vers un autre emplacement. Par exemple, vous pouvez déplacer les données vers des Storage Nodes sur votre grille ou vers un autre Cloud Storage Pool.

Étapes

1. Sélectionnez **ILM > Pools de stockage > Cloud Storage Pools**.

2. Consultez la colonne « Utilisation ILM » du tableau pour déterminer si vous pouvez supprimer le Cloud Storage Pool.

Vous ne pouvez pas supprimer un Cloud Storage Pool s'il est utilisé dans une règle ILM ou dans un profil de codage d'effacement.

3. Si le Cloud Storage Pool est utilisé, sélectionnez ***cloud storage pool name* > ILM usage**.

4. "[Cloner chaque règle ILM](#)" qui place actuellement des objets dans le Cloud Storage Pool que vous souhaitez supprimer.

5. Déterminez où vous souhaitez déplacer les objets existants gérés par chaque règle que vous avez clonée.

Vous pouvez utiliser un ou plusieurs pools de stockage ou un Cloud Storage Pool différent.

6. Modifiez chacune des règles que vous avez clonées.

Pour l'étape 2 de l'assistant de création de règle ILM, sélectionnez le nouvel emplacement dans le champ **copies at**.

7. "[Créer une nouvelle politique ILM](#)" et remplacez chacune des anciennes règles par une règle clonée.

8. Activez la nouvelle stratégie.

9. Attendez qu'ILM retire les objets du Cloud Storage Pool et les place dans le nouvel emplacement.

Supprimer le pool de stockage cloud

Lorsque le Cloud Storage Pool est vide et n'est utilisé dans aucune règle ILM, vous pouvez le supprimer.

Avant de commencer

- Vous avez supprimé toutes les règles ILM qui auraient pu utiliser le pool.
- Vous avez confirmé que le 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 "[Dépanner les pools de stockage cloud](#)".



Lorsque vous créez un pool de stockage cloud, StorageGRID écrit un fichier marqueur dans le compartiment ou le conteneur pour l'identifier comme un pool de stockage cloud. Ne supprimez pas ce fichier, qui porte le nom `x-ntap-sgws-cloud-pool-uuid`.

Étapes

1. Sélectionnez **ILM > Pools de stockage > Cloud Storage Pools**.
2. Si la colonne d'utilisation ILM indique que Cloud Storage Pool n'est pas utilisé, cochez la case.
3. Sélectionnez **Actions > Supprimer**.
4. Sélectionnez **OK**.

Dépanner les pools de stockage cloud dans StorageGRID

Utilisez ces étapes de dépannage pour résoudre les erreurs que vous pourriez rencontrer lors de la création, de la modification ou de la suppression d'un Cloud Storage Pool.

Déterminez si une erreur s'est produite

StorageGRID effectue une vérification de l'état simple sur chaque pool de stockage cloud en lisant l'objet connu `x-ntap-sgws-cloud-pool-uuid` afin de s'assurer que le pool de stockage cloud est accessible et fonctionne correctement. Lorsque StorageGRID rencontre une erreur sur le point de terminaison, il effectue une vérification de l'état chaque minute à partir de chaque nœud de stockage. Lorsque l'erreur est résolue, les vérifications de l'état s'arrêtent. Si une vérification de l'état détecte un problème, un message s'affiche dans la colonne « Dernière erreur » du tableau des pools de stockage cloud sur la page des pools de stockage.

Le tableau présente l'erreur la plus récente détectée pour chaque Cloud Storage Pool et indique depuis combien de temps l'erreur s'est produite.

De plus, une alerte d'erreur de connectivité du Cloud Storage Pool est déclenchée si la vérification de l'état détecte qu'une ou plusieurs nouvelles erreurs de Cloud Storage Pool se sont produites au cours des 5 dernières minutes. Si vous recevez une notification par e-mail concernant cette alerte, accédez à la page **Storage pools** (sélectionnez **ILM > Storage pools**), consultez les messages d'erreur dans la colonne **Last error**, et reportez-vous aux instructions de dépannage ci-dessous.

Vérifiez si une erreur a été résolue

Après avoir résolu les problèmes sous-jacents, vous pouvez déterminer si l'erreur a été résolue. Depuis la page **Cloud Storage Pool**, sélectionnez le point de terminaison, puis sélectionnez **Effacer l'erreur**. Un message de confirmation indique que StorageGRID a effacé l'erreur pour le Cloud Storage Pool.

Si le problème sous-jacent a été résolu, le message d'erreur n'est plus affiché. Cependant, si le problème sous-jacent n'a pas été corrigé (ou si une autre erreur est rencontrée), le message d'erreur s'affichera dans la colonne **Last error** dans quelques minutes.

Erreur : Échec de la vérification de l'état. Erreur du point de terminaison

Vous pouvez rencontrer cette erreur lorsque vous activez le verrouillage d'objets S3 avec la rétention par défaut pour votre compartiment Amazon S3 après avoir commencé à utiliser ce compartiment comme Cloud Storage Pool. Cette erreur se produit lorsque l'opération PUT ne comporte pas d'en-tête HTTP avec une valeur de somme de contrôle de la charge utile telle que `Content-MD5`. Cette valeur d'en-tête est requise par AWS pour les opérations PUT dans les compartiments avec le verrouillage d'objets S3 activé.

Pour corriger ce problème, suivez les étapes dans ["Modifier un pool de stockage cloud"](#) sans apporter de modifications. Cette action déclenche la validation de la configuration du Cloud Storage Pool qui détecte et met à jour automatiquement le flag S3 Object Lock sur la configuration du point de terminaison du Cloud Storage Pool.

Erreur : Ce Cloud Storage Pool contient du contenu inattendu

Vous pouvez rencontrer cette erreur lorsque vous tentez de créer, de modifier ou de supprimer un Cloud Storage Pool. Cette erreur se produit si le bucket ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` fichier marqueur, mais que ce fichier ne contient pas le champ de métadonnées avec l'UUID attendu.

En règle générale, cette erreur ne s'affiche que si vous créez un nouveau Cloud Storage Pool et qu'une autre instance de StorageGRID utilise déjà le même Cloud Storage Pool.

Essayez l'une de ces solutions pour corriger le problème :

- Si vous configurez un nouveau pool de stockage cloud et que le compartiment contient le fichier `x-ntap-sgws-cloud-pool-uuid` et des clés d'objet supplémentaires similaires à l'exemple suivant, créez un nouveau compartiment et utilisez ce nouveau compartiment à la place.

Exemple de clé d'objet supplémentaire : `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si le fichier `x-ntap-sgws-cloud-pool-uuid` est le seul objet dans le compartiment, supprimez ce fichier.

Si ces étapes ne s'appliquent pas à votre situation, contactez le support.

Erreur : Impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du point de terminaison

Vous pourriez rencontrer cette erreur dans les circonstances suivantes :

- Lorsque vous essayez de créer ou de modifier un Cloud Storage Pool.
- Lorsque vous sélectionnez une combinaison de plateforme, d'authentification ou de protocole non prise en charge avec S3 Object Lock lors de la configuration d'un nouveau Cloud Storage Pool. Voir ["Considérations relatives aux pools de stockage cloud"](#).

Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID d'écrire dans le Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur provenant du point de terminaison.

- Si le message d'erreur contient `Get url: EOF`, vérifiez que le point de terminaison de service utilisé pour le Cloud Storage Pool n'utilise pas HTTP pour un conteneur ou un compartiment qui requiert 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 point de terminaison de service utilisé pour le Cloud Storage Pool.
- Si l'erreur est due à une plateforme, une authentification ou un protocole non pris en charge, passez à une configuration prise en charge avec S3 Object Lock et essayez d'enregistrer à nouveau le nouveau Cloud Storage Pool.
- Pour tous les autres messages d'erreur de point de terminaison, essayez une ou plusieurs des solutions suivantes :
 - Créez un conteneur ou un compartiment externe portant le même nom que celui que vous avez saisi pour le Cloud Storage Pool, puis essayez d'enregistrer à nouveau le nouveau Cloud Storage Pool.
 - Corrigez le nom du conteneur ou du compartiment que vous avez spécifié pour le Cloud Storage Pool, puis essayez d'enregistrer à nouveau le nouveau Cloud Storage Pool.

Erreur : Échec de l'analyse du certificat d'autorité de certification

Vous pouvez rencontrer cette erreur lorsque vous tentez de créer ou de modifier un Cloud Storage Pool. Cette erreur se produit si StorageGRID n'a pas pu analyser le certificat que vous avez saisi lors de la configuration du Cloud Storage Pool.

Pour corriger ce problème, vérifiez le certificat d'autorité de certification que vous avez fourni pour détecter d'éventuels problèmes.

Erreur : aucun Cloud Storage Pool avec cet ID n'a été trouvé

Vous pouvez rencontrer cette erreur lorsque vous tentez de modifier ou de supprimer un Cloud Storage Pool. Cette erreur se produit si le point de terminaison renvoie une réponse 404, ce qui peut signifier l'une des choses suivantes :

- Les identifiants utilisés pour le Cloud Storage Pool ne disposent pas des autorisations de lecture pour le compartiment.
- Le compartiment utilisé pour le pool de stockage cloud ne contient pas le `x-ntap-sgws-cloud-pool-uuid` marker file.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée dispose des autorisations requises.

- Modifiez le pool de stockage cloud avec des identifiants disposant des autorisations requises.
- Si les autorisations sont correctes, contactez le support.

Erreur : Impossible de vérifier le contenu du Cloud Storage Pool. Erreur du point de terminaison

Vous pouvez rencontrer cette erreur lorsque vous tentez de supprimer un Cloud Storage Pool. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID de lire le contenu du bucket du Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur provenant du point de terminaison.

Erreur : des objets ont déjà été placés dans ce compartiment

Vous pouvez rencontrer cette erreur lorsque vous tentez de supprimer un Cloud Storage Pool. Vous ne pouvez pas supprimer un Cloud Storage Pool s'il contient des données déplacées par ILM, des données présentes dans le bucket avant la configuration du Cloud Storage Pool, ou des données ajoutées au bucket par une autre source après la création du Cloud Storage Pool.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Suivez les instructions pour déplacer les objets vers StorageGRID dans « Cycle de vie d'un objet Cloud Storage Pool ».
- Si vous êtes certain que les objets restants n'ont pas été placés dans le Cloud Storage Pool par ILM, supprimez manuellement les objets du compartiment.



Ne supprimez jamais manuellement des objets d'un pool de stockage cloud qui y auraient été placés par ILM. Si vous tentez ultérieurement d'accéder à un objet supprimé manuellement depuis StorageGRID, celui-ci sera introuvable.

Erreur : Le proxy a rencontré une erreur externe lors de la tentative d'accès au Cloud Storage Pool

Cette erreur peut survenir si vous avez configuré un proxy de stockage non transparent entre les nœuds de stockage et le point de terminaison S3 externe utilisé pour le Cloud Storage Pool. Cette erreur se produit si le serveur proxy externe ne peut pas atteindre le point de terminaison du Cloud Storage Pool. Par exemple, le serveur DNS pourrait ne pas être en mesure de résoudre le nom d'hôte ou il pourrait y avoir un problème de réseau externe.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Vérifiez les paramètres du Cloud Storage Pool (**ILM > Storage pools**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Erreur : le certificat X.509 est hors de sa période de validité

Vous pouvez rencontrer cette erreur lorsque vous tentez de supprimer un Cloud Storage Pool. Cette erreur se produit lorsque l'authentification requiert un certificat X.509 pour garantir que le bon Cloud Storage Pool externe est validé et que le pool externe est vide avant la suppression de la configuration du Cloud Storage Pool.

Essayez les étapes suivantes pour corriger le problème :

- Mettez à jour le certificat configuré pour l'authentification auprès du Cloud Storage Pool.

- Assurez-vous que toute alerte d'expiration de certificat concernant ce Cloud Storage Pool est résolue.

Informations connexes

["Cycle de vie d'un objet Cloud Storage Pool"](#)

Gérez les profils de code d'effacement dans StorageGRID

Vous pouvez afficher les détails d'un profil de codage à effacement et renommer un profil si nécessaire. Vous pouvez désactiver un profil de codage à effacement s'il n'est pas actuellement utilisé dans des règles ILM.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Afficher les détails du profil de codage d'effacement

Vous pouvez consulter les détails d'un profil de codage d'effacement pour déterminer son statut, le schéma de codage d'effacement utilisé et d'autres informations.

Étapes

1. Sélectionnez **Configuration > Système > Codage d'effacement**.
2. Sélectionnez le profil. La page de détails du profil s'affiche.
3. `${post_edited_translations.segment}`
4. `${post_edited_translations.segment}`

Renommer un profil de codage d'effacement

Vous pourriez renommer un profil de codage d'effacement pour rendre plus évident ce que fait le profil.

Étapes

1. Sélectionnez **Configuration > Système > Codage d'effacement**.
2. Sélectionnez le profil que vous souhaitez renommer.
3. `${post_edited_translations.segment}`
4. Saisissez un nom unique pour le profil de codage d'effacement.

`${post_edited_translations.segment}`



Les noms de profils à 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 codage d'effacement

Vous pouvez désactiver un profil de codage d'effacement si vous ne prévoyez plus de l'utiliser et si le profil n'est actuellement utilisé dans aucune règle ILM.



Vérifiez qu'aucune opération de réparation des données avec codage d'effacement ni aucune procédure de mise hors service n'est en cours. Un message d'erreur est renvoyé si vous tentez de désactiver un profil de codage d'effacement alors que l'une de ces opérations est en cours.

À propos de cette tâche

`${post_edited_translations.segment}`

- Le profil de codage d'effacement est actuellement utilisé dans une règle ILM.
- `${post_edited_translations.segment}`

Étapes

1. Sélectionnez **Configuration > Système > Codage d'effacement**.
2. `${post_edited_translations.segment}`

Il est impossible de désactiver un profil de codage d'effacement s'il est utilisé dans une règle ILM. Dans l'exemple, le profil 2+1 Data Center 1 est utilisé dans au moins une règle ILM.

☐	Profile name ? ⇅	Status ? ⇅	Storage pool ? ⇅	Erasure-coding scheme ? ⇅
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. `${post_edited_translations.segment}`
 - a. Sélectionnez **ILM > Règles**.
 - b. `${post_edited_translations.segment}`
 - c. Si la règle ILM utilise le profil de codage d'effacement que vous souhaitez désactiver, déterminez si la règle est utilisée dans une quelconque stratégie ILM.
 - d. `${post_edited_translations.segment}`

<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	Aucune étape supplémentaire n'est requise. Poursuivez cette procédure.	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	i. Modifiez ou supprimez toutes les règles ILM concernées. Si vous modifiez la règle, supprimez tous les emplacements qui utilisent le profil de codage d'effacement. ii. Poursuivez cette procédure.	<code>"\${post_edited_translations.segment}"</code>

<code>\${post_edited_translation s.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translation s.segment}</code>
Dans une règle ILM qui fait actuellement partie d'une politique ILM active	i. Clonez la politique. ii. <code>\${post_edited_translations.segment}</code> iii. Ajoutez une ou plusieurs nouvelles règles ILM pour garantir la protection des objets. iv. <code>\${post_edited_translations.segment}</code> v. Attendez que la nouvelle politique soit appliquée et que les objets existants soient déplacés vers de nouveaux emplacements selon les nouvelles règles que vous avez ajoutées. <code>\${post_edited_translations.segment}</code> Vous pouvez tenter de désactiver un profil de codage d'effacement sans risque tant qu'il est associé à des données, mais l'opération échouera. Un message d'erreur vous informera si le profil n'est pas encore prêt à être désactivé. vi. Modifiez ou supprimez la règle que vous avez retirée de la politique. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de codage à effacement. vii. Poursuivez cette procédure.	"Créer une politique ILM" "<code>\${post_edited_translation s.segment}</code>"
<code>\${post_edited_translations. segment}</code>	i. <code>\${post_edited_translations.segment}</code> ii. <code>\${post_edited_translations.segment}</code> iii. <code>\${post_edited_translations.segment}</code> iv. Enregistrez la règle. v. Modifiez ou supprimez la règle que vous avez retirée de la politique. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de codage à effacement. vi. Poursuivez cette procédure.	"Créer une politique ILM" "<code>\${post_edited_translation s.segment}</code>"

e. Actualisez la page Profils de codage d'effacement pour vous assurer que le profil n'est pas utilisé dans une règle ILM.

- Si le profil n'est pas utilisé dans une règle ILM, sélectionnez le bouton radio et sélectionnez **Désactiver**. La boîte de dialogue Désactiver le profil de codage d'effacement s'affiche.



Vous pouvez sélectionner plusieurs profils à désactiver simultanément, à condition que chaque profil ne soit utilisé dans aucune règle.

- Si vous êtes sûr de vouloir désactiver le profil, sélectionnez **Désactiver**.

Résultats

- Si StorageGRID parvient à désactiver le profil de codage d'effacement, son statut est Désactivé. Vous ne pouvez plus sélectionner ce profil pour aucune règle ILM. Vous ne pouvez pas réactiver un profil désactivé.
- Si StorageGRID ne parvient pas à désactiver le profil, un message d'erreur s'affiche. Par exemple, un message d'erreur s'affiche si des données d'objet sont toujours associées à ce profil. Il se peut que vous deviez patienter plusieurs semaines avant de réessayer la procédure de désactivation.

Configurer les régions S3 pour StorageGRID

Les règles ILM peuvent filtrer les objets en fonction des régions facultatives où les 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 qui peuvent être utilisées par les compartiments de votre système.



Vous ne pouvez pas changer la région d'un bucket après la création de celui-ci.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

À propos de cette tâche

Lors de la création d'un compartiment S3, vous pouvez spécifier que le compartiment soit créé dans une région spécifique. Spécifier une région permet au compartiment d'être géographiquement proche de ses utilisateurs, ce qui peut aider à optimiser la latence, à minimiser les coûts et à répondre aux exigences réglementaires.

Lorsque vous créez une règle ILM, vous 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`. Vous pouvez ensuite spécifier que des copies de ces objets soient placées sur des nœuds de stockage d'un site de centre de données situé dans cette région afin d'optimiser la latence.

Lors de la configuration des régions, suivez ces instructions :

- Par défaut, tous les compartiments sont considérés comme appartenant à la `us-east-1` région.
- Vous devez créer les régions à l'aide de Grid Manager avant de pouvoir spécifier une région autre que celle par défaut lors de la création de compartiments à l'aide de Tenant Manager ou de l'API de gestion des locataires, ou avec l'élément de requête `LocationConstraint` pour les requêtes d'API S3 PUT Bucket. Une erreur se produit si une requête PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.
- Vous devez utiliser le nom exact de la région lors de la création du compartiment S3. Les noms de région sont sensibles à la casse. Les caractères autorisés sont les chiffres, les lettres et les tirets.



« EU » n'est pas considéré comme un alias pour « eu-west-1 ». Si vous souhaitez utiliser la région « EU » ou « eu-west-1 », vous devez utiliser le nom exact.

- Vous ne pouvez pas supprimer ou modifier une région si elle est utilisée dans une règle attribuée à une stratégie (active ou inactive).

- Si vous utilisez une région non valide comme filtre avancé dans une règle ILM, vous ne pouvez pas ajouter cette règle à une stratégie.

Une région invalide peut se produire si vous utilisez une région comme filtre avancé dans une règle ILM, mais que vous supprimez ultérieurement cette région, ou si vous utilisez l'API de gestion de grille pour créer une règle et spécifier une région que vous n'avez pas définie.

- Si vous supprimez une région après l'avoir utilisée pour créer un compartiment S3, vous devrez la rajouter si vous souhaitez utiliser le filtre avancé Location Constraint pour trouver des objets dans ce compartiment.

Étapes

1. Sélectionnez **ILM > Regions**.

La page Régions s'affiche.

2. Sélectionnez l'onglet **Toutes les régions** ou **Région par défaut**.

Toutes les régions

L'onglet **Toutes les régions** répertorie les régions actuellement définies, y compris la région par défaut définie.



Vous ne pouvez ni supprimer ni modifier la région par défaut dans l'onglet **Toutes les régions**. Utilisez l'onglet **Région par défaut** pour changer la région par défaut.

- a. Pour ajouter une région, sélectionnez **Ajouter une autre région**.
- b. Saisissez le nom d'une région que vous souhaitez utiliser lors de la création de compartiments S3.

Vous devez utiliser exactement ce nom de région comme élément de requête LocationConstraint lors de la création du compartiment S3 correspondant.

- c. Pour supprimer une zone inutilisée, sélectionnez l'icône de suppression .

Un message d'erreur s'affiche si vous tentez de supprimer une région actuellement utilisée dans une stratégie (active ou inactive).

- d. Une fois vos modifications terminées, sélectionnez **Enregistrer**.

Vous pouvez désormais sélectionner ces régions dans la section Filtres avancés de l'étape 1 de l'assistant de création de règle ILM. Voir "[Utilisez les filtres avancés dans les règles ILM](#)".

Région par défaut

L'onglet **Région par défaut** affiche la région par défaut actuellement définie, que vous pouvez modifier.

- a. Pour modifier la région par défaut, sélectionnez le nom de la région parmi les options disponibles dans la liste déroulante **Région par défaut**.
- b. Sélectionnez **Enregistrer**.

Créer une règle ILM

Découvrez les règles ILM dans StorageGRID

Pour gérer les objets, vous créez un ensemble de règles de gestion du cycle de vie de l'information (ILM) et les organisez dans une politique ILM.

Chaque objet ingéré dans le système est évalué au regard de la politique active. Lorsqu'une règle de cette politique correspond aux métadonnées d'un objet, les instructions qu'elle contient déterminent les actions que StorageGRID entreprend pour copier et stocker cet objet.



Les métadonnées des objets ne sont pas gérées par les règles ILM. À la place, les métadonnées des objets sont stockées dans une base de données Cassandra dans ce que l'on appelle un référentiel de métadonnées. Trois copies des métadonnées des objets sont automatiquement conservées sur chaque site afin de protéger les données contre toute perte.

Éléments d'une règle ILM

Une règle ILM comporte trois éléments :

- **Critères de filtrage** : Les filtres de base et avancés d'une règle définissent les objets auxquels la règle s'applique. Si un objet correspond à tous les filtres, StorageGRID applique la règle et crée les copies de l'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'objets. Chaque règle peut inclure une séquence d'instructions de placement permettant de modifier le nombre, le type et l'emplacement des copies d'objets au fil du temps. À l'expiration du délai d'un placement, les instructions du placement suivant sont automatiquement appliquées lors de la prochaine évaluation ILM.
- **Comportement d'ingestion** : Le comportement d'ingestion d'une règle vous permet de choisir comment les objets filtrés par la règle sont protégés lors de leur ingestion (lorsqu'un client S3 enregistre un objet dans la grille).

Filtrage des règles ILM

Lorsque vous créez une règle ILM, vous spécifiez des filtres pour identifier les objets auxquels la règle s'applique.

Dans le cas le plus simple, une règle peut ne pas utiliser de filtres. Toute règle qui ne comporte pas de filtres s'applique à tous les objets ; elle doit donc être la dernière règle (par défaut) d'une stratégie ILM. La règle par défaut fournit des instructions de stockage pour les objets qui ne correspondent pas aux filtres d'une autre règle.

- Les filtres de base permettent d'appliquer des règles différentes à de grands groupes d'objets distincts. Ces filtres permettent d'appliquer une règle à des comptes locataires spécifiques, à des compartiments S3 spécifiques, ou aux deux.

Les filtres de base vous offrent un moyen simple d'appliquer différentes règles à un grand nombre d'objets. Par exemple, les dossiers financiers de votre entreprise peuvent devoir être stockés pour répondre aux exigences réglementaires, tandis que les données du service marketing peuvent devoir être stockées pour faciliter les opérations quotidiennes. Après avoir créé des comptes locataires distincts pour chaque service ou après avoir séparé les données des différents services dans des compartiments S3 distincts, vous pouvez facilement créer une règle qui s'applique à tous les dossiers financiers et une seconde règle qui s'applique à toutes les données marketing.

- Les filtres avancés vous offrent un contrôle précis. Vous pouvez créer des filtres pour sélectionner des objets en fonction des propriétés d'objet suivantes :
 - Temps d'ingestion
 - Dernier temps d'accès
 - Tout ou partie du nom de l'objet (clé)
 - Contrainte de localisation (S3 uniquement)
 - Taille de l'objet
 - Métadonnées utilisateur
 - Balise d'objet (S3 uniquement)

Vous pouvez filtrer les objets selon des critères très précis. Par exemple, les objets stockés par le service d'imagerie d'un hôpital peuvent être fréquemment utilisés lorsqu'ils ont moins de 30 jours, puis plus rarement par la suite, tandis que les objets contenant des informations sur les consultations des patients peuvent devoir être copiés au service de facturation du siège du réseau de santé. Vous pouvez créer des filtres qui identifient chaque type d'objet en fonction du nom de l'objet, de sa taille, des balises d'objet S3 ou de tout autre critère pertinent, puis créer des règles distinctes pour stocker chaque ensemble d'objets de manière appropriée.

Vous pouvez combiner les filtres selon vos besoins au sein d'une même règle. Par exemple, le service marketing peut souhaiter stocker les fichiers image volumineux différemment de leurs dossiers fournisseurs, tandis que le service des ressources humaines peut avoir besoin de stocker les dossiers du personnel dans une zone géographique spécifique et les informations relatives aux politiques de manière centralisée. Dans ce cas, vous pouvez créer des règles qui filtrent par compte locataire afin de séparer les enregistrements de chaque service, tout en utilisant des filtres dans chaque règle pour identifier le type spécifique d'objets auquel la règle s'applique.

Instructions de placement des règles ILM

Les instructions de placement déterminent où, quand et comment les données d'un objet sont stockées. Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps.

Lorsque vous créez des instructions de placement :

- Vous commencez par spécifier l'heure de référence, qui détermine le moment où les instructions de placement commencent. L'heure de référence peut correspondre au moment où un objet est ingéré, au moment où un objet est accédé, au moment où un objet versionné devient non actuel, ou à une heure définie par l'utilisateur.
- Ensuite, vous spécifiez quand le placement s'appliquera, par rapport à la date de référence. Par exemple, un placement peut commencer le jour 0 et se poursuivre pendant 365 jours, par rapport au moment où l'objet a été ingéré.
- Enfin, vous spécifiez le type de copies (réplication ou code d'effacement) et l'emplacement où les copies sont stockées. Par exemple, vous pouvez choisir de stocker deux copies répliquées sur deux sites différents.

Chaque règle peut définir plusieurs emplacements pour une même période et des emplacements différents pour des périodes différentes.

- Pour placer des objets à plusieurs emplacements au cours d'une même période, sélectionnez **Ajouter un autre type ou emplacement** pour ajouter plus d'une ligne pour cette période.
- Pour placer des objets à différents endroits et à différentes périodes, sélectionnez **Ajouter une autre**

période pour ajouter la période suivante. Spécifiez ensuite une ou plusieurs lignes au sein de la période.

L'exemple illustre deux instructions de placement sur la page Définir les placements de l'assistant Créer une règle ILM.

Time period and placements [Sort by start date](#)

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day store for days

Store objects by copies at ,

and store objects by using

[Add other type or location](#)

Time period 2

From Day store forever

Store objects by copies at

[Add other type or location](#)

La première consigne de placement **1** comporte deux lignes pour la première année :

- La première ligne crée deux copies répliquées de l'objet sur deux sites de centres de données.
- La deuxième ligne crée une copie 6+3 avec code d'effacement en utilisant tous les sites des centres de données.

La deuxième instruction de placement **2** crée deux copies après un an et les conserve indéfiniment.

Lorsque vous définissez l'ensemble des instructions de placement pour une règle, vous devez vous assurer qu'au moins une instruction de placement commence au jour 0, qu'il n'y a pas d'intervalles entre les périodes que vous avez définies et que la dernière instruction de placement se poursuit soit indéfiniment, soit jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

À l'expiration de chaque période définie par la règle, les instructions de placement du contenu pour la période suivante sont appliquées. De nouvelles copies d'objets sont créées et toutes les copies inutiles sont supprimées.

Comportement d'ingestion des règles ILM

Le comportement d'ingestion détermine si les copies d'objets sont placées immédiatement conformément aux instructions de la règle, ou si des copies intermédiaires sont créées et les instructions de placement appliquées ultérieurement. Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Équilibré** : StorageGRID tente de créer toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela s'avère impossible, des copies intermédiaires sont créées et un message de succès est renvoyé au

client. Les copies spécifiées dans la règle ILM sont créées dès que possible.

- **Strict** : Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que la réussite ne soit renvoyée au client.
- **Double validation** : StorageGRID crée immédiatement des copies intermédiaires de l'objet et renvoie la réussite au client. Les copies spécifiées dans la règle ILM sont créées lorsque cela est possible.

Informations connexes

- ["Options d'ingestion"](#)
- ["Avantages, inconvénients et limites des options d'ingestion"](#)
- ["Comment la cohérence et les règles ILM interagissent pour affecter la protection des données"](#)

Exemple de règle ILM

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

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

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

Informations connexes

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

Accédez à l'assistant de création de règle ILM dans StorageGRID

Les règles ILM permettent de gérer le placement des données d'objets au fil du temps. Pour créer une règle ILM, vous utilisez l'assistant de création de règle ILM.



Si vous souhaitez créer la règle ILM par défaut pour une stratégie, suivez plutôt ["Instructions pour la création d'une règle ILM par défaut"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Si vous souhaitez spécifier les comptes locataires auxquels cette règle s'applique, vous avez la ["Autorisation d'accès aux comptes locataires"](#) ou vous connaissez l'identifiant de compte pour chaque compte.
- Si vous souhaitez que la règle filtre les objets en fonction des métadonnées du temps d'accès, les mises à jour du temps d'accès doivent être activées par le compartiment S3.

- Vous avez configuré les Cloud Storage Pools que vous prévoyez d'utiliser. Voir ["Créer un pool de stockage cloud"](#).
- Vous connaissez le ["options d'ingestion"](#).
- Si vous devez créer une règle conforme pour une utilisation avec S3 Object Lock, vous connaissez le ["Exigences relatives au verrouillage d'objet S3"](#).
- Vous avez éventuellement visionné la vidéo :

[Aperçu des règles ILM](#)

À propos de cette tâche

Lors de la création de règles ILM :

- Tenez compte de la topologie du système StorageGRID et des configurations de stockage.
- Déterminez le type de copies d'objets que vous souhaitez réaliser (répliquées ou code d'effacement) et le nombre de copies de chaque objet requis.
- Déterminez quels types de métadonnées d'objets sont utilisés dans les applications qui se connectent au système StorageGRID. Les règles ILM filtrent les objets en fonction de leurs métadonnées.
- Réfléchissez à l'endroit où vous souhaitez placer les copies d'objets au fil du temps.
- Choisissez l'option d'ingestion à utiliser (Balanced, Strict ou Dual commit).

Étapes

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez **Créer**. ["Étape 1 \(Saisir les détails\)"](#) de l'assistant Créer une règle ILM apparaît.

Saisissez les détails et les filtres d'une règle ILM StorageGRID

L'étape **Saisir les détails** de l'assistant Créer une règle ILM vous permet de saisir un nom et une description pour la règle et de définir des filtres pour la règle.

La saisie d'une description et la définition de filtres pour la règle sont facultatives.

À propos de cette tâche

Lors de l'évaluation d'un objet par rapport à une ["Règle ILM"](#) règle, StorageGRID compare les métadonnées de l'objet aux filtres de la règle. Si les métadonnées de l'objet correspondent à tous les filtres, StorageGRID utilise la règle pour placer l'objet. Vous pouvez concevoir une règle applicable à tous les objets, ou spécifier des filtres de base, tels qu'un ou plusieurs comptes locataires ou noms de compartiments, ou des filtres avancés, tels que la taille de l'objet ou les métadonnées utilisateur.

Étapes

1. Saisissez un nom unique pour la règle dans le champ **Nom**.
2. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.

Vous devriez décrire l'objectif ou la fonction de la règle afin de pouvoir la reconnaître ultérieurement.

3. Vous pouvez sélectionner un ou plusieurs comptes locataires S3 auxquels cette règle s'applique. Si cette règle s'applique à tous les locataires, laissez ce champ vide.

Si vous ne disposez pas des droits d'accès racine ou des droits d'accès aux comptes locataires, vous ne pouvez pas sélectionner de locataires dans la liste. Saisissez plutôt l'ID du locataire ou plusieurs ID sous

forme de chaîne délimitée par des virgules.

4. Vous pouvez éventuellement spécifier les compartiments S3 auxquels cette règle s'applique.

Si l'option **s'applique à tous les compartiments** est sélectionnée (par défaut), la règle s'applique à tous les compartiments S3.

5. Pour les locataires S3, vous pouvez éventuellement sélectionner **Oui** pour appliquer la règle uniquement aux anciennes versions d'objets dans les compartiments S3 dont le versionnage est activé.

Si vous sélectionnez **Oui**, « Heure non actuelle » sera automatiquement sélectionnée comme heure de référence dans ["Étape 2 de l'assistant de création de règle ILM"](#).



L'horodatage non actuel s'applique uniquement aux objets S3 dans les compartiments compatibles avec le versionnage. Voir ["Opérations sur les compartiments, PutBucketVersioning"](#) et ["Gérez les objets avec S3 Object Lock"](#).

Vous pouvez utiliser cette option pour réduire l'impact sur le stockage des objets versionnés en filtrant les versions d'objets non actuelles. Voir ["Exemple 4 : Règles et politique ILM pour les objets versionnés S3"](#).

6. Vous pouvez également sélectionner **Ajouter un filtre avancé** pour spécifier des filtres supplémentaires.

Si vous ne configurez pas le filtrage avancé, la règle s'applique à tous les objets correspondant aux filtres de base. Pour plus d'informations sur le filtrage avancé, consultez [Utilisez les filtres avancés dans les règles ILM](#) et [Spécifiez plusieurs types et valeurs de métadonnées](#).

7. Sélectionnez **Continuer**. ["Étape 2 \(Définir les placements\)"](#) de l'assistant Créer une règle ILM apparaît.

Utilisez les filtres avancés dans les règles ILM

Le filtrage avancé vous permet de créer des règles ILM qui s'appliquent uniquement à certains objets en fonction de leurs métadonnées. Lorsque vous configurez un filtrage avancé pour une règle, vous sélectionnez le type de métadonnées à prendre en compte, un opérateur et une valeur de métadonnée. Lors de l'évaluation des objets, la règle ILM est appliquée uniquement à ceux dont les métadonnées correspondent au filtre avancé.

Le tableau présente les types de métadonnées que vous pouvez spécifier dans les filtres avancés, les opérateurs que vous pouvez utiliser pour chaque type de métadonnées et les valeurs de métadonnées attendues.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Temps d'ingestion	• est • n'est pas • est avant • est le ou avant • est après • est le ou après	Date et heure d'ingestion de l'objet. Remarque : Pour éviter les problèmes de ressources lors de l'activation d'une nouvelle politique ILM, vous pouvez utiliser le filtre avancé Heure d'acquisition dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez l'Heure d'acquisition sur une valeur supérieure ou égale à l'heure approximative à laquelle la nouvelle politique entrera en vigueur afin de garantir que les objets existants ne soient pas déplacés inutilement.
Clé	• égale • n'est pas égal • contient • ne contient pas • commence par • ne commence pas par • se termine par • ne se termine pas par	Tout ou partie d'une clé d'objet S3 unique. Par exemple, vous pourriez vouloir faire correspondre les objets qui se terminent par <code>.txt</code> ou qui commencent par <code>test-object/</code>.
Dernier temps d'accès	• est • n'est pas • est avant • est le ou avant • est après • est le ou après	Date et heure de la dernière récupération (lecture ou consultation) de l'objet. Remarque : Si vous prévoyez d'"utiliser le dernier temps d'accès" utiliser un filtre avancé, les mises à jour du temps d'accès doivent être activées pour le compartiment S3.
Contrainte de localisation (S3 uniquement)	• égale • n'est pas égal	La région où un compartiment S3 a été créé. Utilisez ILM > Régions pour définir les régions affichées. Remarque : La valeur <code>us-east-1</code> correspondra aux objets des compartiments créés dans la région <code>us-east-1</code> ainsi qu'aux objets des compartiments pour lesquels aucune région n'est spécifiée. Voir "Configurer les régions S3".

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Taille de l'objet	• égale • n'est pas égal • moins que • inférieur ou égal à • supérieur à • supérieur ou égal à	La taille de l'objet. Le code d'effacement est idéal pour les objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets de moins de 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.
Métadonnées utilisateur	• contient • se termine par • égale • existe • commence par • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par	Paire clé-valeur, où Nom des métadonnées utilisateur est la clé et Valeur des métadonnées est la valeur. Par exemple, pour filtrer les objets qui ont des métadonnées utilisateur de <code>color=blue</code>, spécifiez <code>color</code> pour Nom des métadonnées utilisateur, <code>equals</code> pour l'opérateur, et <code>blue</code> pour Valeur des métadonnées. Remarque : Les noms des métadonnées utilisateur ne sont pas sensibles à la casse ; les valeurs des métadonnées utilisateur sont sensibles à la casse.
Balise d'objet (S3 uniquement)	• contient • se termine par • égale • existe • commence par • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par	Paire clé-valeur, où Nom de l'étiquette d'objet est la clé et Valeur de l'étiquette d'objet est 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 la balise d'objet, <code>equals</code> pour l'opérateur et <code>True</code> pour Valeur de la balise d'objet. Remarque : Les noms et valeurs des balises d'objet sont sensibles à la casse. Vous devez saisir ces éléments exactement comme ils ont été définis pour l'objet.

Spécifiez plusieurs types et valeurs de métadonnées

Lorsque vous définissez un filtrage avancé, vous pouvez spécifier plusieurs types de métadonnées et plusieurs valeurs de métadonnées. Par exemple, si vous souhaitez qu'une règle corresponde aux objets dont la taille est comprise entre 10 Mo et 100 Mo, vous devez sélectionner le type de métadonnées **Object size** et spécifier deux valeurs de métadonnées.

- La première valeur de métadonnées spécifie les objets supérieurs ou égaux à 10 Mo.
- La deuxième valeur de métadonnées spécifie les objets inférieurs ou égaux à 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size	greater than or equal to	10	MB	✕
and				
Object size	less than or equal to	100	MB	✕

L'utilisation de plusieurs entrées vous permet de contrôler précisément quels objets sont concernés. Dans l'exemple suivant, la règle s'applique aux objets dont la métadonnée utilisateur camera_type a pour valeur Brand A ou Brand B. Cependant, la règle ne s'applique qu'aux objets Brand B dont la taille est inférieure à 10 Mo.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand A	✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand B	✕
and				
Object size	less than or equal to	10	MB	✕

[Add another advanced filter](#)

Définir les instructions de placement pour une règle StorageGRID ILM

L'étape **Définir les emplacements** de l'assistant Créer une règle ILM vous permet de définir les instructions d'emplacement qui déterminent la durée de stockage des objets, le type de copies (répliquées ou codées par effacement), l'emplacement de stockage et le nombre de copies.



Les captures d'écran présentées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID.

À propos de cette tâche

Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une période de temps unique. Lorsque vous utilisez plusieurs instructions, les périodes doivent être contiguës et au moins une instruction doit commencer au 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 comporter plusieurs lignes si vous souhaitez créer différents types de copies ou utiliser différents emplacements pendant cette période.

Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une autre sur le site 2 pendant la première année. Après un an, une copie à codage d'effacement 2+1 est créée et enregistrée sur un seul site.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Étapes

1. Pour **Heure de référence**, sélectionnez le type d'heure à utiliser pour calculer l'heure de début d'une instruction de placement.

Option	Description
Temps d'ingestion	L'heure à laquelle l'objet a été ingéré.
Dernier temps d'accès	Le moment où l'objet a été récupéré (lu ou consulté) pour la dernière fois. Pour utiliser cette option, la mise à jour du temps d'accès doit être activée pour le compartiment S3. Voir "Utilisez le temps d'accès dans les règles ILM".
heure de création définie par l'utilisateur	Une heure spécifiée dans les métadonnées définies par l'utilisateur.
Temps non actuel	L'option « Heure non actuelle » est automatiquement sélectionnée si vous avez sélectionné Oui à la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le versionnage activé) ? » dans "Étape 1 de l'assistant de création d'une règle ILM" .

Si vous souhaitez créer une règle *conforme*, vous devez sélectionner **Heure d'ingestion**. Reportez-vous à ["Gérez les objets avec S3 Object Lock"](#).

2. Dans la section **Période et affectations**, saisissez une heure de début et une durée pour la première période.

Par exemple, vous pouvez spécifier où stocker les objets pendant la première année (*À partir du jour 0, stocker pendant 365 jours*). Au moins une instruction doit commencer au jour 0.

3. Si vous souhaitez créer des copies répliquées :

- a. Dans la liste déroulante **Stocker les objets par**, sélectionnez **réplication**.
- b. Sélectionnez le nombre de copies que vous souhaitez réaliser.

Un avertissement s'affiche si vous modifiez le nombre de copies à 1. Une règle ILM qui ne crée qu'une seule copie répliquée pour une période donnée expose les données à un risque de perte définitive. Reportez-vous à "[Pourquoi vous ne devriez pas utiliser la réplication à copie unique](#)".

Pour éviter ce risque, effectuez une ou plusieurs des actions suivantes :

- Augmentez le nombre d'exemplaires pour la période concernée.
- Ajoutez des copies à d'autres pools de stockage ou à un Cloud Storage Pool.
- Sélectionnez **code d'effacement** au lieu de **la réplication**.

Vous pouvez ignorer sans risque cet avertissement si cette règle crée déjà plusieurs copies pour toutes les périodes.

- c. Dans le champ **copies à**, sélectionnez les pools de stockage que vous souhaitez ajouter.

Si vous ne spécifiez qu'un seul pool de stockage, sachez que StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si votre grille comprend trois nœuds de stockage et que vous sélectionnez 4 comme nombre de copies, seules trois copies seront créées—une copie par nœud de stockage.

L'alerte **Placement ILM impossible** est déclenchée pour indiquer que la règle ILM n'a pas pu être entièrement appliquée.

Si vous spécifiez plusieurs pools de stockage, gardez ces règles à l'esprit :

- Le nombre de copies ne peut pas être supérieur au nombre de pools de stockage.
- Si le nombre de copies est égal au nombre de pools de stockage, une copie de l'objet est stockée dans chaque pool de stockage.
- Si le nombre de copies est inférieur au nombre de pools de stockage, une copie est stockée sur le site d'ingestion, puis le système répartit les copies restantes afin de maintenir une utilisation équilibrée du disque entre 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 risquent d'être enregistrées sur un seul site. Pour cette raison, ne spécifiez pas le pool de stockage All Storage Nodes (StorageGRID 11.6 et versions antérieures) et un autre pool de stockage.

4. Si vous souhaitez créer une copie avec code d'effacement :

- a. Dans la liste déroulante **Store objects by**, sélectionnez **erasure coding**.



Le code d'effacement est idéal pour les objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets de moins de 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

- b. Si vous n'avez pas ajouté de filtre de taille d'objet pour une valeur supérieure à 200 Ko, sélectionnez **Précédent** pour revenir à l'étape 1. Ensuite, sélectionnez **Ajouter un filtre avancé** et définissez un filtre **Taille d'objet** sur une valeur supérieure à 200 Ko.

- c. Sélectionnez le pool de stockage que vous souhaitez ajouter et le schéma de code d'effacement que vous souhaitez utiliser.

L'emplacement de stockage d'une copie à code d'effacement comprend le nom du schéma de code d'effacement, suivi du nom du pool de stockage.

Les schémas de code d'effacement disponibles sont limités par le nombre de nœuds de stockage dans le pool de stockage que vous sélectionnez. Un **Recommended** badge apparaît à côté des schémas qui fournissent soit le **"meilleure protection ou la charge de stockage la plus faible"**.

5. Facultatif :

- a. Sélectionnez **Ajouter un autre type ou emplacement** pour créer des copies supplémentaires à différents emplacements.
- b. Sélectionnez **Ajouter une autre période** pour ajouter différentes périodes.



La suppression des objets s'effectue selon les paramètres suivants :

- Les objets sont automatiquement supprimés à la fin de la période finale, sauf si une autre période se termine par **forever**.
- Selon **"Paramètres de période de rétention des compartiments et des locataires"** les cas, les objets peuvent ne pas être supprimés même si la période de rétention ILM prend fin.

6. Si vous souhaitez stocker des objets dans un pool de stockage cloud :

- a. Dans la liste déroulante **Stocker les objets par**, sélectionnez **réplication**.
- b. Sélectionnez le champ **copies à**, puis sélectionnez un Cloud Storage Pool.

Lorsque vous utilisez des pools de stockage cloud, gardez ces règles à l'esprit :

- Vous ne pouvez pas sélectionner plusieurs Cloud Storage Pool dans une même instruction de placement. De même, vous ne pouvez pas sélectionner à la fois un Cloud Storage Pool et un pool de stockage dans la même instruction de placement.
- Vous ne pouvez stocker qu'une seule copie d'un objet dans un Cloud Storage Pool donné. Un message d'erreur s'affiche si vous définissez **Copies** sur 2 ou plus.
- Vous ne pouvez pas stocker plus d'une copie d'objet dans un même Cloud Storage Pool en même temps. Un message d'erreur s'affiche si plusieurs placements utilisant un Cloud Storage Pool ont des dates qui se chevauchent ou si plusieurs lignes dans le même placement utilisent un Cloud Storage Pool.
- Vous pouvez stocker un objet dans un Cloud Storage Pool en même temps que cet objet est stocké sous forme de copies répliquées ou à code d'effacement dans StorageGRID. Cependant, vous devez inclure plus d'une ligne dans l'instruction de placement pour la période concernée, afin de pouvoir spécifier le nombre et les types de copies pour chaque emplacement.

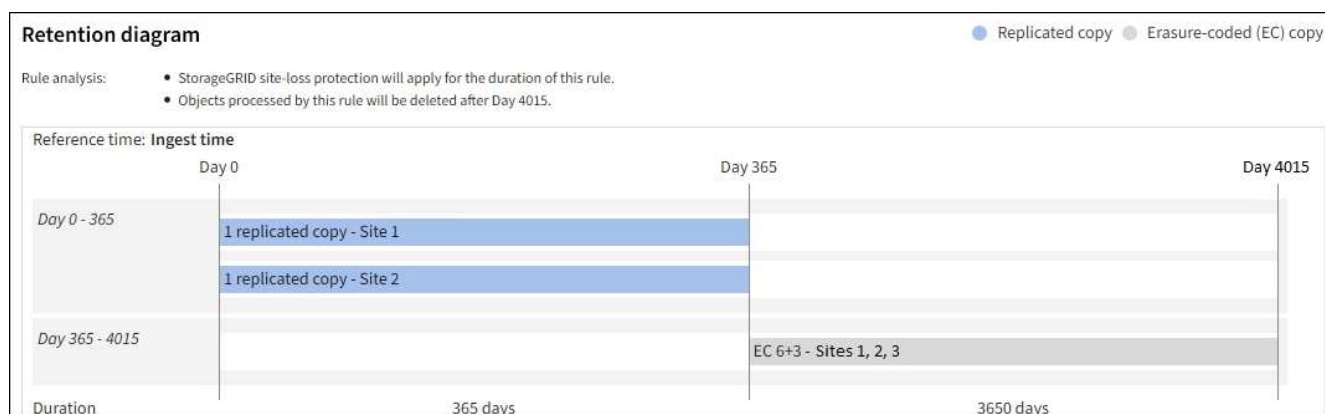
7. Dans le schéma de rétention, confirmez vos instructions de placement.

Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une autre sur le site 2 pendant la première année. Après un an et pendant dix années supplémentaires, une copie 6+3 avec code d'effacement sera enregistrée sur trois sites. Après un total de onze ans, les objets seront supprimés de StorageGRID.

La section « Analyse des règles » du diagramme de rétention indique :

- La protection contre les pertes de site de StorageGRID s'appliquera pendant toute la durée de cette règle.
- Les objets traités par cette règle seront supprimés après le 4015e jour.

Consultez ["Activez la protection contre la perte du site."](#)



- Sélectionnez **Continuer**. ["Étape 3 \(Sélectionnez le comportement d'ingestion\)"](#) de l'assistant Créer une règle ILM s'affiche.

Utiliser le temps d'accès dans les règles ILM de StorageGRID

Vous pouvez utiliser le temps d'accès comme référence dans une règle ILM. Par exemple, vous pouvez conserver les objets consultés au cours des trois derniers mois sur les nœuds de stockage locaux, tout en déplaçant les objets qui n'ont pas été consultés aussi récemment vers un emplacement distant. Vous pouvez également utiliser le temps d'accès comme filtre avancé si vous souhaitez qu'une règle ILM s'applique uniquement aux objets consultés pour la dernière fois à une date précise.

À propos de cette tâche

Avant d'utiliser le temps d'accès dans une règle ILM, examinez les considérations suivantes :

- Lorsque vous utilisez le temps d'accès comme référence, sachez que la modification du temps d'accès pour un objet ne déclenche pas une évaluation ILM immédiate. À la place, les placements de l'objet sont évalués et l'objet est déplacé si nécessaire lorsque l'ILM en arrière-plan évalue l'objet. Cela peut prendre deux semaines ou plus après l'accès à l'objet.

Tenez compte de cette latence lors de la création de règles ILM basées sur le temps d'accès et évitez les placements qui utilisent des périodes courtes (moins d'un mois).

- Lorsque vous utilisez le temps d'accès comme filtre avancé ou comme heure de référence, vous devez activer la mise à jour du temps d'accès pour les compartiments S3. Vous pouvez utiliser le ["Gestionnaire de locataires"](#) ou le ["API de gestion des locataires"](#).



La mise à jour du temps d'accès est désactivée par défaut pour les compartiments S3.



Notez que l'activation de la mise à jour du temps d'accès peut réduire les performances, notamment sur les systèmes contenant des objets de petite taille. Cette baisse de performance est due au fait que StorageGRID doit mettre à jour les objets avec un nouvel horodatage à chaque fois qu'ils sont récupérés.

Le tableau suivant récapitule si le temps d'accès est mis à jour pour tous les objets du compartiment pour différents types de requêtes.

Type de demande	Si le temps d'accès est mis à jour lorsque les mises à jour du temps d'accès sont désactivées	Indique si le temps d'accès est mis à jour lorsque les mises à jour du 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
Demande de copie d'un objet d'un bucket à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Sélectionnez le comportement d'ingestion pour une règle ILM StorageGRID

L'étape **Sélectionner le comportement d'ingestion** de l'assistant Créer une règle ILM vous permet de choisir comment les objets filtrés par cette règle sont protégés lors de leur ingestion.

À propos de cette tâche

StorageGRID peut effectuer des copies intermédiaires et mettre les objets en file d'attente pour une évaluation ILM ultérieure, ou il peut effectuer des copies pour respecter immédiatement les instructions de placement de la règle.

Étapes

1. Sélectionnez "[comportement d'ingestion](#)" à utiliser.

Pour plus d'informations, consultez "[Avantages, inconvénients et limites des options d'ingestion](#)".

Vous ne pouvez pas utiliser l'option Équilibré ou Strict si la règle utilise l'un de ces placements :



- Un pool de stockage cloud au jour 0
- Un pool de stockage cloud lorsque la règle utilise une date de création définie par l'utilisateur comme heure de référence

Voir "[Exemple 5 : Règles et politique ILM pour le comportement d'ingestion strict](#)".

2. Sélectionnez **Create**.

La règle ILM est créée. La règle ne devient active que lorsqu'elle est ajoutée à une "[Règle ILM](#)" et que cette stratégie est activée.

Pour consulter les détails de la règle, sélectionnez le nom de la règle sur la page des règles ILM.

Créez une règle ILM par défaut dans StorageGRID

Avant de créer une stratégie ILM, vous devez créer une règle par défaut pour placer tous les objets non couverts par une autre règle dans la stratégie. La règle par défaut ne peut utiliser aucun filtre. Elle doit s'appliquer à tous les locataires, tous les compartiments et toutes les versions d'objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

À propos de cette tâche

La règle par défaut est la dernière à être évaluée dans une stratégie ILM, elle ne peut donc pas utiliser de filtres. Les instructions de placement de la règle par défaut s'appliquent à tous les objets qui ne sont pas couverts par une autre règle de la stratégie.

Dans cet exemple de politique, la première règle s'applique uniquement aux objets appartenant à test-tenant-1. La règle par défaut, qui est la dernière, s'applique aux objets appartenant à tous les autres comptes tenant.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Lors de la création de la règle par défaut, tenez compte des exigences suivantes :

- La règle par défaut sera automatiquement placée en dernière position lorsque vous l'ajoutez à une politique.
- La règle par défaut ne peut utiliser aucun filtre de base ni aucun filtre avancé.
- La règle par défaut doit s'appliquer à toutes les versions de l'objet.
- La règle par défaut doit créer des copies répliquées.



N'utilisez pas comme règle par défaut une règle créant des copies avec codage d'effacement. Les règles de codage d'effacement doivent utiliser un filtre avancé pour empêcher le codage d'effacement des petits objets.

- En général, la règle par défaut devrait conserver les objets indéfiniment.
- Si vous utilisez (ou prévoyez d'activer) le paramètre global de verrouillage des objets S3, la règle par défaut doit être conforme.

Étapes

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez **Create**.

L'étape 1 (Saisir les détails) de l'assistant de création de règle ILM apparaît.

3. Saisissez un nom unique pour la règle dans le champ **Rule name**.
4. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.
5. Laissez le champ **Comptes locataires** vide.

La règle par défaut doit s'appliquer à tous les comptes locataires.

6. Laissez la sélection du menu déroulant Nom du compartiment sur **s'applique à tous les compartiments**.

La règle par défaut doit s'appliquer à tous les compartiments S3.

7. Conservez la réponse par défaut, **Non**, à la question : « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le versionnage activé) ? »

8. N'ajoutez pas de filtres avancés.

La règle par défaut ne peut spécifier aucun filtre.

9. Sélectionnez **Next**.

L'étape 2 (Définir les emplacements) apparaît.

10. Pour l'heure de référence, sélectionnez une option.

Si vous avez conservé la réponse par défaut, **Non**, à la question « Appliquer cette règle uniquement aux anciennes versions de l'objet » Le temps non actuel ne sera pas inclus dans la liste déroulante. La règle par défaut doit s'appliquer à toutes les versions de l'objet.

11. Spécifiez les instructions de placement pour la règle par défaut.

- La règle par défaut devrait conserver les objets indéfiniment. Un avertissement s'affiche lors de l'activation d'une nouvelle stratégie si la règle par défaut ne conserve pas les objets indéfiniment. Vous devez confirmer que ce comportement est bien celui que vous attendez.
- La règle par défaut doit créer des copies répliquées.



N'utilisez pas comme règle par défaut une règle créant des copies avec codage d'effacement. Les règles de codage d'effacement doivent inclure le filtre avancé **Taille de l'objet (Mo) supérieure à 200 Ko** afin d'empêcher le codage d'effacement des objets de petite taille.

- Si vous utilisez (ou prévoyez d'activer) le paramètre global de verrouillage des objets S3, la règle par défaut doit être conforme :
 - Il doit créer au moins deux copies d'objet répliquées ou une copie codée par effacement.
 - Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne des instructions de placement.
 - Il est impossible d'enregistrer des copies d'objets dans un Cloud Storage Pool.
 - Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant l'heure d'ingestion comme référence temporelle.
 - Au moins une ligne des instructions de placement doit être « forever ».

12. Consultez le schéma de rétention pour confirmer vos instructions de placement.

13. Sélectionnez **Continue**.

L'étape 3 (Sélectionner le comportement d'ingestion) apparaît.

14. Sélectionnez l'option d'ingestion à utiliser, puis sélectionnez **Créer**.

Gérer les politiques ILM

Découvrez les politiques ILM dans StorageGRID

Une politique de gestion du cycle de vie de l'information (ILM) est un ensemble ordonné de règles ILM qui détermine comment le système StorageGRID gère les données d'objets au fil du temps.



Une politique ILM incorrectement 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. Confirmez toujours que la politique ILM fonctionnera comme prévu.

`${post_edited_translations.segment}`

Lorsque vous installez StorageGRID et ajoutez des sites, une stratégie ILM par défaut est automatiquement créée, comme suit :

- Si votre grille ne contient qu'un seul site, la politique par défaut contient une règle par défaut qui réplique deux copies de chaque objet sur ce site.
- `${post_edited_translations.segment}`

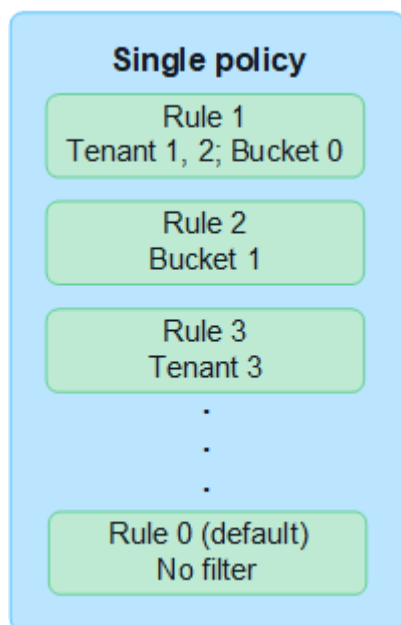
Si la politique par défaut ne répond pas à vos exigences de stockage, vous pouvez créer vos propres règles et politiques. Consultez ["Créer une règle ILM"](#) et ["Créer une politique ILM"](#).

`${post_edited_translations.segment}`

Vous pouvez avoir une ou plusieurs politiques ILM actives simultanément.

`${post_edited_translations.segment}`

Si votre grille utilise un schéma de protection des données simple avec peu de règles spécifiques aux locataires et aux compartiments, utilisez une seule politique ILM active. Les règles ILM peuvent contenir des filtres pour gérer différents compartiments ou locataires.



Lorsqu'une seule stratégie est en place et que les besoins d'un locataire évoluent, vous devez créer une nouvelle stratégie ILM ou cloner la stratégie existante pour appliquer les modifications, effectuer une simulation, puis activer la nouvelle stratégie ILM. Les modifications apportées à la stratégie ILM peuvent entraîner des déplacements d'objets qui peuvent prendre plusieurs jours et provoquer une latence système.

Plusieurs règles

Pour proposer différentes options de qualité de service aux locataires, vous pouvez avoir plusieurs politiques actives à la fois. Chaque politique peut gérer des locataires, des compartiments S3 et des objets spécifiques. Lorsque vous appliquez ou modifiez une politique pour un ensemble spécifique de locataires ou d'objets, les politiques appliquées aux autres locataires et objets ne sont pas affectées.

`${post_edited_translations.segment}`

Si vous souhaitez permettre aux locataires de basculer facilement entre plusieurs politiques de protection des données par compartiment, utilisez plusieurs politiques ILM avec des *étiquettes de politique ILM*. Vous attribuez chaque politique ILM à une étiquette, puis les locataires étiquettent un compartiment pour lui appliquer cette politique. Vous pouvez définir des étiquettes de politique ILM uniquement sur les compartiments S3.

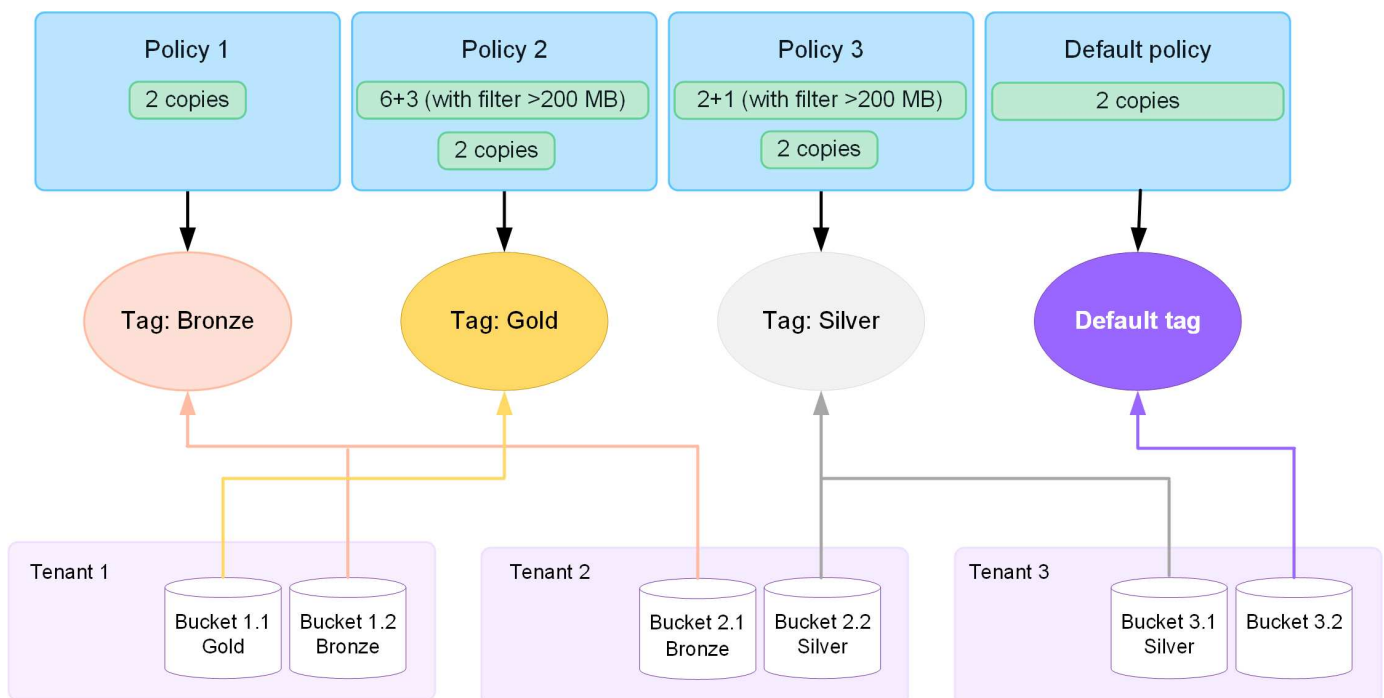
Par exemple, vous pouvez avoir trois étiquettes nommées Gold, Silver et Bronze. Vous pouvez attribuer une stratégie ILM à chaque étiquette, en fonction de la durée et de l'endroit où cette stratégie stocke les objets. Les locataires peuvent choisir la stratégie à utiliser en étiquetant leurs compartiments. Un compartiment étiqueté Gold est géré par la stratégie Gold et bénéficie du niveau de protection des données et de performance Gold.



Vous pouvez "`${post_edited_translations.segment}`" pour votre grille.

Étiquette de stratégie ILM par défaut

Une étiquette de stratégie ILM par défaut est automatiquement créée lors de l'installation de StorageGRID. Chaque grille doit avoir une stratégie active qui est associée à l'étiquette Default. La stratégie par défaut s'applique à tous les compartiments S3 non étiquetés.



Comment une politique ILM évalue-t-elle les objets ?

Une politique ILM active contrôle l'emplacement, la durée et la protection des données des objets.

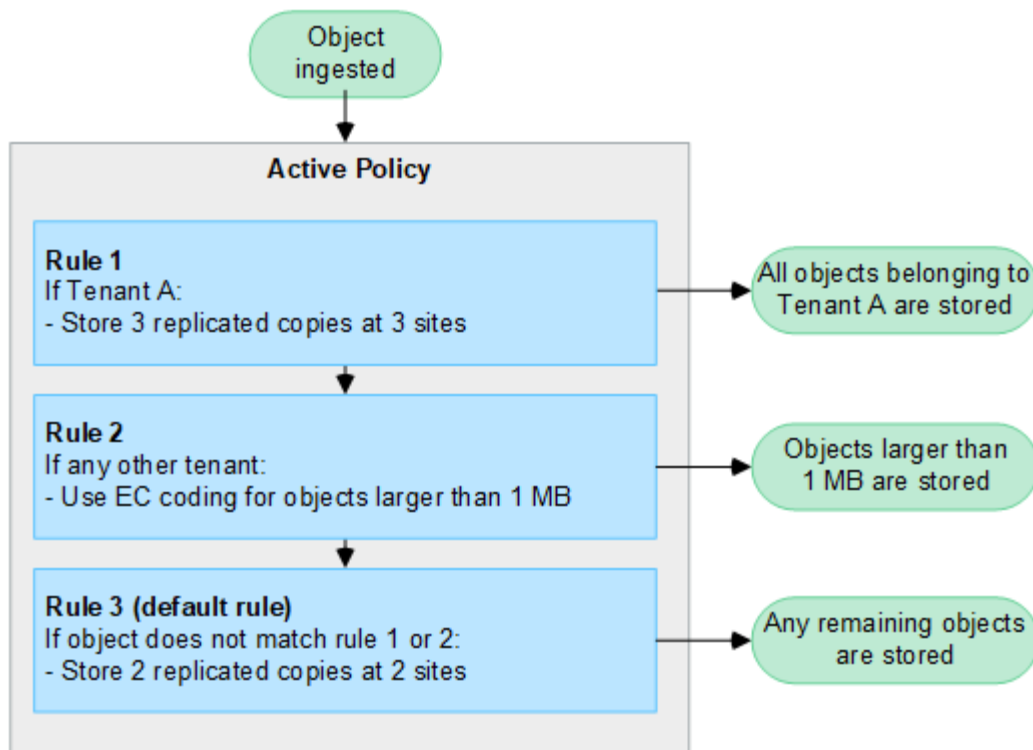
Lorsque les clients enregistrent des objets dans StorageGRID, ces objets sont évalués par rapport à l'ensemble ordonné de règles ILM de la politique, comme suit :

1. Si les filtres de la première règle de la politique correspondent à un objet, celui-ci est ingéré conformément au comportement d'ingestion de cette règle et stocké conformément aux instructions de placement de cette règle.
2. Si les filtres de la première règle ne correspondent pas à l'objet, l'objet est évalué par rapport à chaque règle suivante de la politique jusqu'à ce qu'une correspondance soit trouvée.
3. Si aucune règle ne correspond à un objet, le comportement d'ingestion et les instructions de placement de la règle par défaut de la stratégie sont appliqués. La règle par défaut est la dernière règle de la stratégie. La règle par défaut doit s'appliquer à tous les locataires, tous les compartiments S3 et toutes les versions d'objets, et ne peut utiliser aucun filtre avancé.

`${post_edited_translations.segment}`

À titre d'exemple, une politique ILM pourrait contenir trois règles ILM qui spécifient ce qui suit :

- `${post_edited_translations.segment}`
 - Faites correspondre tous les objets appartenant au locataire A.
 - Stockez ces objets sous forme de trois copies répliquées sur trois sites.
 - `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
 - Faites correspondre tous les objets des autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus volumineux sont stockés à l'aide d'un code d'effacement 6+3 sur trois sites.
 - Ne correspond pas aux objets de 1 Mo ou moins, ces objets sont donc évalués par rapport à la règle 3.
- **Règle 3 : 2 copies 2 centres de données** (par défaut)
 - Est la dernière règle et la règle par défaut de la politique. N'utilise pas de filtres.
 - Créez deux copies répliquées de tous les objets non correspondants à la règle 1 ou à la règle 2 (objets n'appartenant pas à Tenant A et dont la taille est inférieure ou égale à 1 Mo).



Que sont les politiques actives et inactives ?

Chaque système StorageGRID doit avoir au moins une politique ILM active. Si vous souhaitez avoir plus d'une politique ILM active, vous créez des balises de politique ILM et attribuez une politique à chaque balise. Les locataires appliquent ensuite les balises aux compartiments S3. La politique par défaut est appliquée à tous les objets des compartiments auxquels aucune balise de politique n'est attribuée.

Lorsque vous créez une politique ILM pour la première fois, vous sélectionnez une ou plusieurs règles ILM et les organisez dans un ordre spécifique. Après avoir simulé la politique pour confirmer son comportement, vous l'activez.

Lorsque vous activez une politique ILM, StorageGRID utilise cette politique pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Les objets existants peuvent être déplacés vers de nouveaux emplacements lors de la mise en œuvre des règles ILM de la nouvelle politique.

Si vous activez plusieurs stratégies ILM simultanément et que les locataires appliquent des balises de stratégie aux compartiments S3, les objets de chaque compartiment sont gérés en fonction de la stratégie attribuée à la balise.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Utilisez uniquement la stratégie fournie par le système, la stratégie Baseline 2 copies, dans les systèmes de test. Pour StorageGRID 11.6 et versions antérieures, la règle Make 2 Copies de cette stratégie utilise le pool de stockage All Storage Nodes, qui contient tous les sites. Si votre système StorageGRID comporte plus d'un site, deux copies d'un objet peuvent être placées sur le même site.



Le pool de stockage All Storage Nodes est automatiquement créé lors de l'installation de StorageGRID 11.6 et versions antérieures. Si vous effectuez une mise à niveau vers une version ultérieure de StorageGRID, le pool All Storage Nodes existera toujours. Si vous installez StorageGRID 11.7 ou version ultérieure en tant que nouvelle installation, le pool All Storage Nodes n'est pas créé.

- Lors de la conception d'une nouvelle politique, tenez compte de tous les types d'objets susceptibles d'être intégrés à votre grille. Assurez-vous que la politique inclut des règles permettant d'identifier et de placer ces objets comme requis.
- Veillez à ce que la politique ILM soit aussi simple que possible. Cela permet d'éviter les situations potentiellement dangereuses où les données des objets ne sont pas protégées comme prévu lorsque des modifications sont apportées au système StorageGRID au fil du temps.
- Assurez-vous que les règles de la politique sont dans l'ordre correct. Lorsque la politique est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, en commençant par le haut. Par exemple, si la première règle d'une politique correspond à un objet, cet objet ne sera évalué par aucune autre règle.
- La dernière règle de chaque politique ILM est la règle ILM par défaut, qui ne peut utiliser aucun filtre. Si un objet ne correspond à aucune autre règle, la règle par défaut détermine l'emplacement de cet objet et sa durée de conservation.
- Avant d'activer une nouvelle politique, examinez toutes les modifications que la politique apporte à l'emplacement des objets existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

Créer des règles ILM dans StorageGRID

Créez une ou plusieurs politiques ILM pour répondre à vos exigences en matière de qualité de service.

Le fait de disposer d'une seule politique ILM active vous permet d'appliquer les mêmes règles ILM à tous les locataires et compartiments.

Le fait de disposer de plusieurs politiques ILM actives vous permet d'appliquer les règles ILM appropriées à des locataires et des compartiments spécifiques afin de répondre à de multiples exigences de qualité de service.

Créer une politique ILM

À propos de cette tâche

Avant de créer votre propre politique, vérifiez que la ["politique ILM par défaut"](#) ne répond pas à vos besoins de stockage.



Dans les systèmes de test, utilisez uniquement les politiques système fournies, 2 copies Policy (pour les grilles à un seul site) ou 1 Copy per Site (pour les grilles multi-sites). Pour StorageGRID 11.6 et versions antérieures, la règle par défaut de cette politique utilise le pool de stockage All Storage Nodes, qui contient tous les sites. Si votre système StorageGRID comporte plusieurs sites, deux copies d'un objet peuvent être placées sur le même site.



Si le ["Le paramètre global de verrouillage des objets S3 a été activé"](#) cas se présente, vous devez vous assurer que la stratégie ILM est conforme aux exigences des compartiments pour lesquels S3 Object Lock est activé. Dans cette section, suivez les instructions qui mentionnent que S3 Object Lock est activé.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).
- Vous avez ["règles ILM créées"](#) selon que le verrouillage d'objet S3 est activé ou non.

Verrouillage d'objet S3 non activé

- Vous avez ["créé les règles ILM"](#) que vous souhaitez ajouter à la politique. Selon vos besoins, vous pouvez enregistrer une politique, créer des règles supplémentaires, puis modifier la politique pour y ajouter les nouvelles règles.
- Vous avez ["a créé une règle ILM par défaut"](#) qui ne contient aucun filtre.

Verrouillage d'objet S3 activé

- Le ["Le paramètre global de verrouillage des objets S3 est déjà activé"](#) pour le système StorageGRID.
- Vous avez ["créé les règles ILM conformes et non conformes"](#) que vous souhaitez ajouter à la politique. Au besoin, vous pouvez enregistrer une politique, créer des règles supplémentaires, puis modifier la politique pour y ajouter les nouvelles règles.
- Vous avez ["a créé une règle ILM par défaut"](#) pour la politique conforme.

- Vous avez éventuellement visionné la vidéo :

Aperçu des politiques ILM

Voir aussi ["Utilisez les politiques ILM"](#).

Étapes

1. Sélectionnez **ILM > Politiques**.

Si le paramètre global S3 Object Lock est activé, la page des stratégies ILM indique quelles règles ILM sont conformes.

2. Déterminez comment vous souhaitez créer la politique ILM.

Créer une nouvelle règle

- a. Sélectionnez **Créer une politique**.

Cloner la politique existante

- a. Cochez la case correspondant à la stratégie avec laquelle vous souhaitez commencer, puis sélectionnez **Clone**.

Modifier la politique existante

- a. Si une politique est inactive, vous pouvez la modifier. Cochez la case correspondant à la politique inactive avec laquelle vous souhaitez commencer, puis sélectionnez **Modifier**.

3. Dans le champ **Nom de la stratégie**, saisissez un nom unique pour la stratégie.
4. Facultativement, dans le champ **Motif de la modification**, saisissez la raison pour laquelle vous créez une nouvelle règle.
5. Pour ajouter des règles à la stratégie, sélectionnez **Sélectionner les règles**. Sélectionnez un nom de règle pour afficher les paramètres de cette règle.

Si vous clonez une règle :

- Les règles utilisées par la politique que vous clonez sont sélectionnées.
- Si la politique que vous clonez utilisait des règles sans filtre qui n'étaient pas la règle par défaut, vous êtes invité à supprimer toutes ces règles sauf une.
- Si la règle par défaut utilisait un filtre, vous êtes invité à sélectionner une nouvelle règle par défaut.
- Si la règle par défaut n'était pas la dernière règle, vous pouvez déplacer la règle à la fin de la nouvelle politique.

Verrouillage d'objet S3 non activé

- a. Sélectionnez une règle par défaut pour la stratégie. Pour créer une nouvelle règle par défaut, sélectionnez la **page des règles ILM**.

La règle par défaut s'applique à tous les objets qui ne correspondent à aucune autre règle de la stratégie. La règle par défaut ne peut utiliser aucun filtre et est toujours évaluée en dernier.



N'utilisez pas la règle « Créer 2 copies » comme règle par défaut pour une stratégie. La règle « Créer 2 copies » utilise un seul pool de stockage, « Tous les nœuds de stockage », qui contient tous les sites. Si votre système StorageGRID comporte plusieurs sites, deux copies d'un objet peuvent être placées sur le même site.

Verrouillage d'objet S3 activé

- a. Sélectionnez une règle par défaut pour la stratégie. Pour créer une nouvelle règle par défaut, sélectionnez la **page des règles ILM**.

La liste des règles contient uniquement les règles conformes et n'utilise aucun filtre.



N'utilisez pas la règle « Créer 2 copies » comme règle par défaut d'une stratégie. La règle « Créer 2 copies » utilise un seul pool de stockage, All Storage Nodes, qui contient tous les sites. Si vous utilisez cette règle, plusieurs copies d'un objet peuvent être placées sur le même site.

- b. Si vous avez besoin d'une règle « par défaut » différente pour les objets dans des compartiments S3 non conformes, sélectionnez **Inclure une règle sans filtre pour les compartiments S3 non conformes**, puis sélectionnez une règle non conforme qui n'utilise pas de filtre.

Par exemple, vous pouvez utiliser un Cloud Storage Pool pour stocker des objets dans des compartiments qui n'ont pas le verrouillage d'objets S3 activé.



Vous ne pouvez sélectionner qu'une seule règle non conforme qui n'utilise pas de filtre.

Voir aussi ["Exemple 7 : Stratégie ILM conforme pour S3 Object Lock"](#).

6. Lorsque vous avez terminé de sélectionner la règle par défaut, sélectionnez **Continuer**.
7. À l'étape « Autres règles », sélectionnez toutes les autres règles que vous souhaitez ajouter à la stratégie. Ces règles utilisent au moins un filtre (compte locataire, nom de compartiment, filtre avancé ou la référence temporelle Noncurrent). Sélectionnez ensuite **Sélectionner**.

La fenêtre « Créer une stratégie » affiche désormais les règles que vous avez sélectionnées. La règle par défaut se trouve à la fin, avec les autres règles au-dessus.

Si le verrouillage d'objet S3 est activé et que vous avez également sélectionné une règle « par défaut » non conforme, cette règle est ajoutée comme avant-dernière règle dans la stratégie.



Un avertissement s'affiche si une règle ne conserve pas les objets indéfiniment. Lorsque vous activez cette stratégie, vous devez confirmer que vous souhaitez que StorageGRID supprime les objets lorsque les instructions de placement de la règle par défaut expirent (sauf si le cycle de vie d'un compartiment conserve les objets pendant une période plus longue).

8. Faites glisser les lignes correspondant aux règles non par défaut pour déterminer l'ordre dans lequel ces règles seront évaluées.

Vous ne pouvez pas déplacer la règle par défaut. Si S3 Object Lock est activé, vous ne pouvez pas non plus déplacer la règle « default » non conforme, le cas échéant.



Vous devez vérifier que les règles ILM sont dans le bon ordre. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, en commençant par le haut.

9. Au besoin, sélectionnez **Select rules** pour ajouter ou supprimer des règles.
10. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
11. Répétez ces étapes pour créer des politiques ILM supplémentaires.
12. [Simuler une politique ILM](#). Vous devez toujours simuler une politique avant de l'activer afin de vous assurer qu'elle fonctionne comme prévu.

Simuler une règle

Simulez une politique sur des objets de test avant d'activer la politique et de l'appliquer à vos données de production.

Avant de commencer

- Vous connaissez le compartiment S3/la clé d'objet pour chaque objet que vous souhaitez tester.

Étapes

1. Utilisez un client S3 ou le ["Console S3"](#), ingérez les objets nécessaires pour tester chaque règle.
2. Sur la page des politiques ILM, cochez la case correspondant à la politique, puis sélectionnez **Simuler**.
3. Dans le champ **Objet**, saisissez le S3 bucket/object-key pour un objet de test. Par exemple, bucket-01/filename.png.
4. Si le versionnage S3 est activé, vous pouvez éventuellement saisir un ID de version pour l'objet dans le champ **ID de version**.
5. Sélectionnez **Simuler**.
6. Dans la section Résultats de la simulation, vérifiez que chaque objet a bien été associé à la règle appropriée.
7. Pour déterminer le pool de stockage ou le profil de code d'effacement en vigueur, sélectionnez le nom de la règle correspondante pour accéder à la page de détails de la règle.



Vérifiez toute modification apportée à l'emplacement des objets répliqués et à code d'effacement existants. Le déplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lors de l'évaluation et de la mise en œuvre des nouveaux emplacements.

Résultats

Toute modification apportée aux règles de la stratégie sera prise en compte dans les résultats de la simulation et affichera la nouvelle correspondance ainsi que la correspondance précédente. La fenêtre de simulation de stratégie conserve les objets testés jusqu'à ce que vous sélectionniez **Tout effacer** ou l'icône de suppression  pour chaque objet dans la liste des résultats de la simulation.

Informations connexes

["Exemples de simulations de politiques ILM"](#)

Activer une règle

Lorsque vous activez une seule nouvelle stratégie ILM, les objets existants et les objets nouvellement ingérés sont gérés par cette stratégie. Lorsque vous activez plusieurs stratégies, les balises de stratégie ILM attribuées aux compartiments déterminent les objets à gérer.

Avant d'activer une nouvelle règle :

1. Simulez la politique pour confirmer qu'elle se comporte comme prévu.
2. Vérifiez toute modification apportée à l'emplacement des objets répliqués et à code d'effacement existants. Le déplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lors de l'évaluation et de la mise en œuvre des nouveaux emplacements.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irrécupérable.

À propos de cette tâche

Lorsque vous activez une stratégie ILM, le système distribue la nouvelle stratégie à tous les nœuds. Cependant, la nouvelle stratégie active peut ne pas entrer en vigueur tant que tous les nœuds de la grille ne sont pas disponibles pour recevoir la nouvelle stratégie. Dans certains cas, le système attend avant de mettre en œuvre une nouvelle stratégie active afin de garantir que les objets de la grille ne soient pas supprimés accidentellement. Plus précisément :

- Si vous apportez des modifications aux politiques qui **augmentent la redondance ou la durabilité des données**, ces modifications s'appliquent immédiatement. Par exemple, si vous activez une nouvelle politique qui inclut une règle de trois copies au lieu d'une règle de deux copies, cette politique s'appliquera immédiatement car elle augmente la redondance des données.
- Si vous apportez des modifications aux règles qui **pourraient diminuer la redondance ou la durabilité des données**, ces modifications ne seront pas appliquées tant que tous les nœuds du grid ne seront pas disponibles. Par exemple, si vous activez une nouvelle règle qui utilise la règle de deux copies au lieu de celle de trois copies, la nouvelle règle apparaîtra dans l'onglet Active policy, mais elle ne prendra effet que lorsque tous les nœuds seront en ligne et disponibles.

Étapes

Suivez les étapes pour activer une ou plusieurs politiques :

Activer une stratégie

Suivez ces étapes si vous n'aurez qu'une seule règle active. Si vous avez déjà une ou plusieurs règles actives et que vous activez des règles supplémentaires, suivez les étapes pour l'activation de plusieurs règles.

1. Lorsque vous êtes prêt à activer une politique, sélectionnez **ILM > Politiques**.

Vous pouvez également activer une seule politique à partir de la page **ILM > Policy tags**.

2. Dans l'onglet Politiques, cochez la case correspondant à la politique que vous souhaitez activer, puis sélectionnez **Activer**.
3. Suivez l'étape appropriée :
 - Si un message d'avertissement vous invite à confirmer que vous souhaitez activer la règle, sélectionnez **OK**.
 - Si un message d'avertissement contenant des détails sur la politique apparaît :
 - i. Vérifiez les détails pour vous assurer que la politique gérera les données comme prévu.
 - ii. Si la règle par défaut conserve les objets pendant un nombre limité de jours, consultez le diagramme de rétention, puis saisissez ce nombre de jours dans la zone de texte.
 - iii. Si la règle par défaut stocke les objets indéfiniment, mais qu'une ou plusieurs autres règles ont une durée de conservation limitée, tapez **oui** dans la zone de texte.
 - iv. Sélectionnez **Activer la stratégie**.

Activer plusieurs règles

Pour activer plusieurs stratégies, vous devez créer des étiquettes de stratégie et attribuer une stratégie à chaque étiquette. Vous pouvez créer un maximum de 10 étiquettes de stratégie pour votre grille.



Lorsque plusieurs balises de stratégie sont utilisées, si les locataires réaffectent fréquemment des balises de stratégie aux compartiments, les performances de la grille peuvent être affectées. Si vous avez des locataires non fiables, envisagez d'utiliser uniquement la balise de stratégie Default.

1. Sélectionnez **ILM > Policy tags**.
2. Sélectionnez **Create**.
3. Dans la boîte de dialogue Créer une balise de stratégie, saisissez un nom de balise et, éventuellement, une description pour la balise.



Les noms et descriptions des balises sont visibles par les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de stratégie à attribuer à leurs compartiments. Par exemple, si la stratégie attribuée supprime les objets après une certaine période, vous pouvez l'indiquer dans la description. N'incluez pas d'informations sensibles dans ces champs.

4. Sélectionnez **Créer une étiquette**.
5. Dans le tableau des balises de stratégie ILM, utilisez le menu déroulant pour sélectionner une stratégie à attribuer à la balise.
6. Si des avertissements apparaissent dans la colonne Limitations de la politique, sélectionnez **Afficher les détails de la politique** pour consulter la politique.

7. Assurez-vous que chaque politique gère les données comme prévu.
8. Sélectionnez **Activer les stratégies attribuées**. Ou sélectionnez **Effacer les modifications** pour supprimer l'attribution de stratégie.
9. Dans la boîte de dialogue « Activer les stratégies avec de nouvelles balises », examinez les descriptions de la manière dont chaque balise, stratégie et règle gèrera les objets. Apportez les modifications nécessaires pour que les stratégies gèrent les objets comme prévu.
10. Lorsque vous êtes certain de vouloir activer les politiques, tapez **oui** dans la zone de texte, puis sélectionnez **Activer les politiques**.

Informations connexes

"Exemple 6 : Modification d'une politique ILM"

Exemples de simulations de stratégies ILM dans StorageGRID

Les exemples de simulations de politiques ILM fournissent des lignes directrices pour structurer et modifier les simulations pour votre environnement.

Exemple 1 : Vérifiez les règles lors de la simulation d'une politique ILM

Cet exemple décrit comment vérifier les règles lors de la simulation d'une politique.

Dans cet exemple, la **stratégie ILM d'exemple** est simulée sur les objets ingérés dans deux compartiments. La stratégie comprend trois règles, comme suit :

- La première règle, **Deux exemplaires, deux ans pour bucket-a**, s'applique uniquement aux objets de bucket-a.
- La deuxième règle, **Objets EC > 1 Mo**, s'applique à tous les compartiments mais filtre les objets supérieurs à 1 Mo.
- La troisième règle, **Deux copies, deux centres de données**, est la règle par défaut. Elle n'inclut aucun filtre et n'utilise pas la référence temporelle Noncurrent.

Après avoir simulé la politique, confirmez que chaque objet a été associé à la règle correcte.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched ?	Previous match ?	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	X
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	X
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	X

Dans cet exemple :

- bucket-a/bucket-a object.pdf`a correctement correspondu à 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 correspondait donc pas à la première règle. En revanche, il a été correctement identifié par la seconde règle, qui filtre les objets de plus de 1 Mo.
- `bucket-b/test object less than 1 MB.pdf`N'ayant pas été prise en compte par les filtres des deux premières règles, elle sera placée selon la règle par défaut, qui ne comporte aucun filtre.

Exemple 2 : Réorganiser les règles lors de la simulation d'une politique ILM

Cet exemple montre comment réorganiser les règles pour modifier les résultats lors de la simulation d'une politique.

Dans cet exemple, la politique **Demo** est simulée. Cette politique, conçue pour trouver les objets ayant des métadonnées utilisateur series=x-men, comprend trois règles, comme suit :

- La première règle, **PNGs**, filtre les noms de clés qui se terminent par .png.
- La deuxième règle, **X-men**, s'applique uniquement aux objets pour le locataire A et filtre les `series=x-men`métadonnées utilisateur.
- La dernière règle, **Deux copies, deux centres de données**, est la règle par défaut, qui correspond à tous les objets qui ne correspondent pas aux deux premières règles.

Étapes

1. Après avoir ajouté les règles et enregistré la politique, sélectionnez **Simuler**.
2. Dans le champ **Objet**, saisissez le bucket S3/la clé d'objet pour un objet de test et sélectionnez **Simuler**.

Les résultats de la simulation apparaissent, montrant que l' `Havok.png`objet a été identifié par la règle **PNGs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Cependant, Havok.png il s'agissait de tester la règle des **X-men**.

3. Pour résoudre ce problème, réorganisez les règles.
 - a. Sélectionnez **Terminer** pour fermer la fenêtre Simulate ILM Policy.
 - b. Sélectionnez **Modifier** pour modifier la politique.
 - c. Faites glisser la règle **X-men** en haut de la liste.
 - d. Sélectionnez **Enregistrer**.
4. Sélectionnez **Simuler**.

Les objets que vous avez testés précédemment sont réévalués par rapport à la politique mise à jour, et les

nouveaux résultats de simulation sont affichés. Dans l'exemple, la colonne Rule matched indique que l'`Havok.png` objet correspond désormais à la règle de métadonnées X-men, comme prévu. La colonne Previous match indique que la règle PNGs correspondait à l'objet lors de la simulation précédente.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	✕

Exemple 3 : Corriger une règle lors de la simulation d’une règle ILM

Cet exemple montre comment simuler une politique, corriger une règle dans la politique et poursuivre la simulation.

Dans cet exemple, la stratégie **Demo** est simulée. Cette stratégie vise à identifier les objets qui ont `series=x-men` des métadonnées utilisateur. Cependant, des résultats inattendus sont survenus lors de la simulation de cette stratégie sur l'objet `Beast.jpg`. Au lieu de correspondre à la règle de métadonnées X-men, l'objet a correspondu à la règle par défaut, `Two copies two data centers`.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	✕

Lorsqu’un objet de test ne correspond pas à la règle attendue dans la politique, vous devez examiner chaque règle de la politique et corriger toute erreur.

Étapes

- Sélectionnez **Terminer** pour fermer la boîte de dialogue Simuler la stratégie. Sur la page de détails de la stratégie, sélectionnez **Diagramme de rétention**. Ensuite, sélectionnez **Développer tout** ou **Afficher les détails** pour chaque règle selon les besoins.
- Vérifiez le compte du locataire de la règle, la date de référence et les critères de filtrage.

Par exemple, supposons que les métadonnées de la règle X-men aient été saisies comme « x-men01 » au lieu de « x-men ».

- Pour résoudre l’erreur, corrigez la règle comme suit :
 - Si la règle fait partie de la politique, vous pouvez soit cloner la règle, soit la supprimer de la politique, puis la modifier.
 - Si la règle fait partie de la politique active, vous devez la cloner. Vous ne pouvez ni modifier ni supprimer une règle de la politique active.

4. Effectuez à nouveau la simulation.

Dans cet exemple, la règle X-men corrigée correspond désormais à l'objet `Beast.jpg` en fonction des `series=x-men` métadonnées utilisateur, comme prévu.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all 				
Object 	Version ID 	Rule matched  	Previous match  	Actions
photos/Beast.jpg	—	X-men	—	

Gérer les balises de stratégie ILM dans StorageGRID

Vous pouvez consulter les détails des balises de politique ILM, modifier une balise ou supprimer une balise.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["autorisations d'accès requises"](#).

Afficher les détails de l'étiquette de la règle ILM

Pour afficher les détails d'une étiquette :

1. Sélectionnez **ILM > Policy tags**.
2. Sélectionnez le nom de la politique dans le tableau. La page de détails de l'étiquette s'affiche.
3. Sur la page de détails, consultez l'historique précédent des stratégies attribuées.
4. Affichez une règle en la sélectionnant.

Modifier l'étiquette de la règle ILM



Les noms et descriptions des balises sont visibles par les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de stratégie à attribuer à leurs compartiments. Par exemple, si la stratégie attribuée supprime les objets après une certaine période, vous pouvez l'indiquer dans la description. N'incluez pas d'informations sensibles dans ces champs.

Pour modifier la description d'une étiquette existante :

1. Sélectionnez **ILM > Policy tags**.
2. Cochez la case correspondant à l'étiquette, puis sélectionnez **Modifier**.

Vous pouvez également sélectionner le nom de l'étiquette. La page de détails de l'étiquette s'affiche et vous pouvez sélectionner **Modifier** sur cette page.

3. Modifiez la description de l'étiquette selon les besoins

4. Sélectionnez **Enregistrer**.

Supprimer le tag de stratégie ILM

Lorsque vous supprimez une étiquette de stratégie, la stratégie Default sera appliquée à tous les compartiments auxquels cette étiquette a été attribuée.

Pour supprimer une étiquette :

1. Sélectionnez **ILM > Policy tags**.
2. Cochez la case correspondant à l'étiquette, puis sélectionnez **Supprimer**. Une boîte de dialogue de confirmation apparaît.

Vous pouvez également sélectionner le nom de l'étiquette. La page de détails de l'étiquette s'affiche, et vous pouvez sélectionner **Remove** sur cette page.

3. Sélectionnez **Oui** pour supprimer le tag.

Informations connexes

["Découvrez comment créer des balises de stratégie ILM"](#)

Vérifiez une stratégie ILM avec la recherche de métadonnées d'objet dans StorageGRID

Après avoir activé une stratégie ILM, ingérez des objets de test représentatifs dans le système StorageGRID, puis effectuez une recherche de métadonnées d'objet pour confirmer que les copies sont effectuées comme prévu et placées aux emplacements corrects.

Avant de commencer

Vous disposez d'un identifiant d'objet, qui peut être l'un des suivants :

- **UUID** : L'identifiant unique universel de l'objet.
- **CBID** : Identifiant unique de l'objet dans StorageGRID. Vous pouvez obtenir le CBID d'un objet à partir du journal des audits. Saisissez le CBID en majuscules.
- **Compartiment S3 et clé d'objet** : Lorsqu'un objet est ingéré via l'interface S3, l'application cliente utilise une combinaison de compartiment et de clé d'objet pour stocker et identifier l'objet. Si le compartiment S3 est versionné 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 de version**.

Étapes

1. Ingérez l'objet.
2. Sélectionnez **ILM > Recherche de métadonnées d'objet**.
3. Saisissez l'identifiant de l'objet dans le champ **Identifiant**. Vous pouvez saisir un UUID, un CBID ou une clé de compartiment/objet S3.
4. Vous pouvez également saisir un ID de version pour l'objet (S3 uniquement).
5. Sélectionnez **Rechercher**.

Les résultats de la recherche de métadonnées de l'objet s'affichent. Cette page répertorie les types d'informations suivants :

- Les métadonnées système, telles que l'identifiant de l'objet (UUID), le type de résultat (objet, marqueur de suppression, compartiment S3) et la taille logique de l'objet. Consultez la capture d'écran ci-dessous pour plus de détails.
- Toutes les paires clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur d'étiquette d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objets dans un Cloud Storage Pool, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multipart, une liste des segments d'objet comprenant les identifiants de segment et les tailles de données. Pour les objets comportant plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées des objets au format de stockage interne non traité. Ces métadonnées brutes incluent des métadonnées système internes dont la persistance d'une version à l'autre n'est pas garantie.

6. Vérifiez que l'objet est stocké au(x) bon(s) emplacement(s) et qu'il s'agit du type de copie approprié.

Si l'option Audit est activée, vous pouvez également surveiller le journal des audits pour le message ORLM Object Rules Met. Le message d'audit ORLM peut vous fournir plus d'informations sur l'état du processus d'évaluation ILM, mais il ne peut pas vous donner d'informations sur l'exactitude du placement des données d'objet ou sur l'exhaustivité de la politique ILM. Vous devez évaluer cela vous-même. Pour plus de détails, voir "[Examiner les journaux d'audit](#)".

L'exemple suivant montre les résultats de la recherche de métadonnées d'un objet de test S3 stocké sous forme de deux copies répliquées.



La capture d'écran ci-dessous est un exemple. Vos résultats varieront en fonction de votre version de StorageGRID.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ) CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIIS": "2",

```

Informations connexes

["Utilisez l'API REST S3"](#)

Travaillez avec les règles ILM et les politiques ILM dans StorageGRID

À mesure que vos besoins de stockage évoluent, vous devrez peut-être mettre en place des politiques supplémentaires ou modifier les règles ILM associées à une politique. Vous pouvez consulter les indicateurs ILM pour évaluer les performances du système.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).

Consultez les politiques ILM

`${post_edited_translations.segment}`

1. Sélectionnez **ILM > Politiques**.
2. Sélectionnez **Stratégies** pour afficher une liste des stratégies actives et inactives. Le tableau indique le nom de chaque stratégie, les étiquettes auxquelles la stratégie est attribuée, ainsi que si la stratégie est active ou inactive.
3. Sélectionnez **Historique d'activation** pour afficher une liste des dates de début et de fin d'activation des stratégies.
4. `#{post_edited_translations.segment}`



Si vous consultez les détails d'une politique dont le statut est Modifié ou Supprimé, un message s'affiche expliquant que vous consultez la version de la politique qui était active pendant la période spécifiée et qui a depuis été modifiée ou supprimée.

`#{post_edited_translations.segment}`

Vous pouvez uniquement modifier une politique inactive. Si vous souhaitez modifier une politique active, désactivez-la ou créez un clone et modifiez-le.

Pour modifier une politique :

1. Sélectionnez **ILM > Politiques**.
2. `#{post_edited_translations.segment}`
3. Modifiez la politique en suivant les instructions figurant dans ["Créer des politiques ILM"](#).
4. Simulez la politique avant de la réactiver.



Une politique ILM incorrectement 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. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Cloner une politique ILM

`#{post_edited_translations.segment}`

1. Sélectionnez **ILM > Politiques**.
2. Cochez la case correspondant à la politique que vous souhaitez cloner, puis sélectionnez **Cloner**.
3. Créez une nouvelle politique à partir de la politique que vous avez clonée en suivant les instructions de ["Créer des politiques ILM"](#).



Une politique ILM incorrectement 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. Confirmez toujours que la politique ILM fonctionnera comme prévu.

`#{post_edited_translations.segment}`

Vous ne pouvez supprimer une politique ILM que si elle est inactive. Pour supprimer une politique :

1. Sélectionnez **ILM > Politiques**.

2. Cochez la case correspondant à la politique inactive que vous souhaitez supprimer.
3. Sélectionnez **Remove**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez le nom de la règle dont vous souhaitez afficher les détails. Exemple :

2 copies 2 data centers

Compliant: No
Ingest behavior: Strict
Reference time: Noncurrent time

Clone Edit Remove

Rule detail Used in policies

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool

Rule analysis: Objects processed by this rule will not be deleted by ILM.

Reference time: Noncurrent time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Data Center 1

EC 2+1 - Data Center 1

Duration Forever

Replicated copy Erasure-coded (EC) copy

De plus, vous pouvez utiliser la page de détails pour cloner, modifier ou supprimer une règle. Vous ne pouvez pas modifier ou supprimer une règle si elle est utilisée dans une politique.

Cloner une règle ILM

Vous pouvez cloner une règle existante si vous souhaitez créer une nouvelle règle qui utilise certains des paramètres de la règle existante. Si vous devez modifier une règle utilisée dans une politique, vous devez plutôt cloner la règle et apporter des modifications au clone. Après avoir apporté des modifications au clone, vous pouvez supprimer la règle d'origine de la politique et la remplacer par la version modifiée, selon vos besoins.



`${post_edited_translations.segment}`

Étapes

1. Sélectionnez **ILM > Règles**.
2. Cochez la case correspondant à la règle que vous souhaitez dupliquer, puis sélectionnez **Cloner**. Vous

pouvez également sélectionner le nom de la règle, puis sélectionner **Cloner** depuis la page de détails de la règle.

3. Mettez à jour la règle clonée en suivant les étapes pour [modification d'une règle ILM](#) et "[\\${post_edited_translations.segment}](#)".

Lors du clonage d'une règle ILM, vous devez saisir un nouveau nom.

Modifier une règle ILM

[\\${post_edited_translations.segment}](#)

Vous ne pouvez pas modifier une règle si elle est utilisée dans une politique ILM. À la place, vous pouvez [cloner la règle](#) et apporter les modifications requises à la copie clonée.



Une politique ILM incorrectement 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. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Étapes

1. Sélectionnez **ILM > Règles**.
2. Vérifiez que la règle que vous souhaitez modifier n'est utilisée dans aucune stratégie ILM.
3. Si la règle que vous souhaitez modifier n'est pas utilisée, cochez la case correspondante et sélectionnez **Actions > Modifier**. Vous pouvez également sélectionner le nom de la règle, puis sélectionner **Modifier** sur la page de détails de la règle.
4. Effectuez les étapes de l'assistant Modifier une règle ILM. Si nécessaire, suivez les étapes pour "[création d'une règle ILM](#)" et "[\\${post_edited_translations.segment}](#)".

Lors de la modification d'une règle ILM, vous ne pouvez pas en changer le nom.

[\\${post_edited_translations.segment}](#)

Pour que la liste des règles ILM actuelles reste gérable, supprimez les règles ILM que vous n'êtes pas susceptible d'utiliser.

Étapes

[\\${post_edited_translations.segment}](#)

1. Clonez la politique.
2. Supprimez la règle ILM du clone de stratégie.
3. Enregistrez, simulez et activez la nouvelle stratégie pour vous assurer que les objets sont protégés comme prévu.
4. [\\${post_edited_translations.segment}](#)

Pour supprimer une règle ILM actuellement utilisée dans une stratégie inactive :

1. [\\${post_edited_translations.segment}](#)
2. Supprimez la règle ILM de la stratégie ou [supprimer la règle](#).
3. Accédez aux étapes pour supprimer une règle ILM qui n'est pas actuellement utilisée.

`${post_edited_translations.segment}`

1. Sélectionnez **ILM > Règles**.
2. Vérifiez que la règle que vous souhaitez supprimer n'est utilisée dans aucune politique.
3. Si la règle que vous souhaitez supprimer n'est pas utilisée, sélectionnez la règle et sélectionnez **Actions > Supprimer**. Vous pouvez sélectionner plusieurs règles et les supprimer toutes en même temps.
4. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Vous pouvez consulter les indicateurs de performance d'ILM, tels que le nombre d'objets dans la file d'attente et le taux d'évaluation. Vous pouvez surveiller ces indicateurs pour déterminer les performances du système. Une file d'attente ou un taux d'évaluation élevés peuvent indiquer que le système ne parvient pas à suivre le rythme d'ingestion, que la charge des applications clientes est excessive ou qu'une condition anormale existe.

Étapes

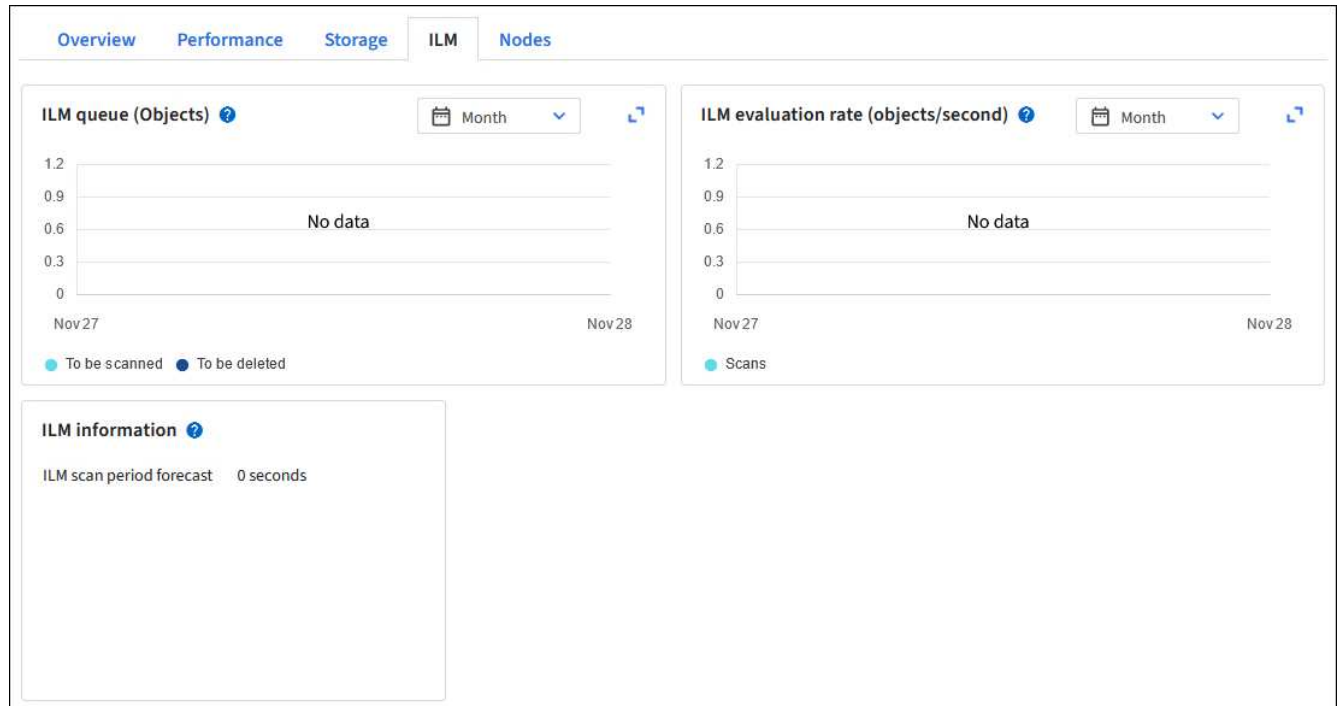
1. Sélectionnez **Tableau de bord > ILM**.



Étant donné que le tableau de bord est personnalisable, l'onglet ILM peut ne pas être disponible.

2. Surveillez les indicateurs de l'onglet ILM.

Vous pouvez sélectionner le point d'interrogation (?) pour afficher une description des éléments de l'onglet ILM.



Utilisez le verrouillage d'objet S3

Comment le verrouillage d'objets S3 protège les objets dans StorageGRID

En tant qu'administrateur de grille, vous pouvez activer le verrouillage d'objets S3 pour votre système StorageGRID et mettre en œuvre une politique ILM conforme afin de garantir que les objets dans des compartiments S3 spécifiques ne soient pas supprimés ou écrasés pendant une période déterminée.

Qu'est-ce que le S3 Object Lock ?

La fonctionnalité StorageGRID S3 Object Lock est une solution de protection des objets équivalente à S3 Object Lock dans Amazon Simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage des objets S3 est activé pour un système StorageGRID, un compte locataire S3 peut créer des compartiments avec ou sans verrouillage des objets S3 activé. Si un compartiment a le verrouillage des objets S3 activé, le versionnage du compartiment est requis et est activé automatiquement.

Un bucket sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne disposera de paramètres de rétention.

Un compartiment avec S3 Object Lock peut contenir des objets avec ou sans paramètres de rétention définis par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un compartiment avec S3 Object Lock et une rétention par défaut configurée peut contenir des objets chargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car la rétention n'a pas été configurée au niveau de l'objet.

En pratique, tous les nouveaux objets ingérés se voient attribuer des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de rétention d'objet restent inchangés.

Modes de rétention

La fonctionnalité StorageGRID S3 Object Lock prend en charge deux modes de rétention pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de rétention Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte.
- En mode gouvernance :
 - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les requêtes pour modifier certains paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation des versions d'objets

Si un compartiment est créé avec le verrouillage d'objets S3 activé, les utilisateurs peuvent utiliser l'application cliente S3 pour spécifier, en option, les paramètres de rétention suivants pour chaque objet ajouté au

compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Retain-until-date** : Si la retain-until-date d'une version d'objet est future, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin d'appliquer une conservation légale à un objet lié à une enquête ou à un litige. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les conservations légales sont indépendantes de la date limite de conservation.



Si un objet fait l'objet d'une rétention légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, voir ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#).

Paramètre de rétention par défaut pour les compartiments

Si un compartiment est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent éventuellement spécifier les paramètres par défaut suivants pour le compartiment :

- **Mode de conservation par défaut** : conformité ou gouvernance.
- **Durée de conservation par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à compter du jour où elles sont ajoutées.

Les paramètres par défaut des compartiments s'appliquent uniquement aux nouveaux objets qui ne possèdent pas leurs propres paramètres de rétention. Les objets existants dans les compartiments ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir ["Créez un compartiment S3"](#) et ["Mettre à jour la rétention par défaut de S3 Object Lock"](#).

Comparaison du verrouillage d'objets S3 à la conformité héritée

Le verrouillage d'objets S3 remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID. Parce que la fonctionnalité de verrouillage d'objets S3 est conforme aux exigences d'Amazon S3, elle rend obsolète la fonctionnalité propriétaire de conformité de StorageGRID, désormais appelée « conformité héritée ».



Le paramètre de conformité global est obsolète. Si vous avez activé ce paramètre dans une version précédente de StorageGRID, le paramètre de verrouillage des objets S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, consultez ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#).

Si vous avez utilisé l'ancienne fonctionnalité de conformité dans une version précédente de StorageGRID, reportez-vous au tableau suivant pour savoir comment elle se compare à la fonctionnalité S3 Object Lock dans StorageGRID.

	Verrouillage d'objet S3	Conformité (legacy)
Comment cette fonctionnalité est-elle activée globalement ?	Dans le Gestionnaire de grille, sélectionnez Configuration > Système > S3 Object Lock .	N'est plus prise en charge.
Comment la fonctionnalité est-elle activée pour un bucket ?	Les utilisateurs doivent activer le verrouillage d'objet S3 lors de la création d'un nouveau compartiment à l'aide de Tenant Manager, de l'API de gestion des locataires ou de l'API REST S3.	N'est plus prise en charge.
Le versionnage des compartiments est-il pris en charge ?	Oui. Le versionnage des compartiments est requis et est activé automatiquement lorsque le verrouillage d'objets S3 est activé pour le compartiment.	Non.
Comment la rétention des objets est-elle définie ?	Les utilisateurs peuvent définir une date limite de conservation pour chaque version d'objet, ou ils peuvent définir une période de conservation par défaut pour chaque compartiment.	Les utilisateurs doivent définir une période de rétention pour l'ensemble du compartiment. La période de rétention s'applique à tous les objets du compartiment.
La durée de conservation peut-elle être modifiée ?	• En mode conformité, la date de conservation d'une version d'objet peut être augmentée, mais jamais diminuée. • En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent réduire, voire supprimer, les paramètres de conservation d'un objet.	La période de rétention d'un bucket peut être augmentée, mais jamais diminuée.
Où le contrôle de la conservation légale est-il effectué ?	Les utilisateurs peuvent imposer ou lever une restriction légale pour toute version d'objet dans le bucket.	Une saisie légale est appliquée au seau et affecte tous les objets dans le seau.

	Verrouillage d'objet S3	Conformité (legacy)
Quand les objets peuvent-ils être supprimés ?	- En mode conformité, une version d'objet peut être supprimée une fois la date limite de conservation atteinte, à condition que l'objet ne soit pas sous séquestre légal. - En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent supprimer un objet avant que sa date de conservation ne soit atteinte, à condition que l'objet ne soit pas sous séquestre légal.	Un objet peut être supprimé après l'expiration de sa période de rétention, à condition que le compartiment ne soit pas soumis à une procédure de conservation légale. Les objets peuvent être supprimés automatiquement ou manuellement.
La configuration du cycle de vie des compartiments est-elle prise en charge ?	Oui	Non

Workflow de verrouillage d'objet S3 dans StorageGRID

`$_post_edited_translations.segment`



L'application des paramètres locataires à l'ensemble de la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état des nœuds et des opérations Cassandra.

Les listes suivantes destinées aux administrateurs de grille et aux utilisateurs locataires contiennent les tâches de haut niveau pour l'utilisation de la fonctionnalité de verrouillage d'objet S3.

Administrateur de grille

- Activez le paramètre de verrouillage global des objets S3 pour l'ensemble du système StorageGRID.
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes*; c'est-à-dire qu'elles répondent aux ["exigences relatives aux compartiments avec S3 Object Lock activé"](#).
- Au besoin, autorisez un locataire à utiliser le mode Conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Au besoin, définissez une période de rétention maximale pour un locataire.

Utilisateur locataire

- Examinez les points à prendre en compte pour les compartiments et les objets avec S3 Object Lock.
- Au besoin, contactez l'administrateur de la grille pour activer le paramètre de verrouillage global S3 Object Lock et définir les autorisations.
- Créez des compartiments avec la fonctionnalité S3 Object Lock activée.
- Vous pouvez également configurer les paramètres de rétention par défaut d'un compartiment :
 - Mode de rétention par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du grid.
 - Durée de conservation par défaut : doit être inférieure ou égale à la durée de conservation maximale définie par l'administrateur du grid.

- Utilisez l'application cliente S3 pour ajouter des objets et, éventuellement, définir une durée de conservation spécifique à chaque objet :
 - Mode de conservation. Gouvernance ou conformité, si autorisé par l'administrateur du grid.
 - À conserver jusqu'à cette date : doit être inférieure ou égale à la durée de conservation maximale autorisée par l'administrateur du grid.

Exigences de S3 Object Lock dans StorageGRID

Vous devez examiner les exigences relatives à l'activation du paramètre global S3 Object Lock, les exigences relatives à la création de règles ILM et de politiques ILM conformes, ainsi que les restrictions que StorageGRID impose aux compartiments et aux objets qui utilisent S3 Object Lock.

Conditions requises pour l'utilisation du paramètre de verrouillage d'objet S3 global

- Vous devez activer le paramètre global S3 Object Lock à l'aide de Grid Manager ou de l'API de gestion de Grid avant que tout locataire S3 puisse créer un compartiment avec S3 Object Lock activé.
- L'activation du paramètre global S3 Object Lock permet à tous les comptes locataires S3 de créer des compartiments avec S3 Object Lock activé.
- Une fois que vous avez activé le paramètre de verrouillage global des objets S3, vous ne pouvez plus le désactiver.
- Vous ne pouvez pas activer le verrouillage global des objets S3 à moins que la règle par défaut dans toutes les stratégies ILM actives ne soit *conforme* (c'est-à-dire que la règle par défaut doit être conforme aux exigences des compartiments avec le verrouillage des objets S3 activé).
- Lorsque le verrouillage global des objets S3 est activé, vous ne pouvez ni créer de nouvelle stratégie ILM ni activer une stratégie ILM existante à moins que la règle par défaut de cette stratégie ne soit conforme. Après l'activation du verrouillage global des objets S3, les pages des règles et des stratégies ILM indiquent quelles règles ILM sont conformes.

Exigences relatives aux règles ILM conformes

Pour activer le verrouillage global des objets S3, vous devez vous assurer que la règle par défaut de toutes les stratégies ILM actives est conforme. Une règle conforme satisfait aux exigences des compartiments pour lesquels le verrouillage des objets S3 est activé, ainsi qu'à celles des compartiments existants pour lesquels la conformité héritée est activée :

- Il doit créer au moins deux copies d'objet répliquées ou une copie codée par effacement.
- Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne des instructions de placement.
- Il est impossible d'enregistrer des copies d'objets dans un Cloud Storage Pool.
- Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant **Ingest time** comme heure de référence.
- Au moins une ligne des instructions de placement doit être « forever ».

Exigences relatives aux politiques ILM

Lorsque le paramètre de verrouillage global des objets S3 est activé, les stratégies ILM actives et inactives peuvent inclure des règles conformes et non conformes.

- La règle par défaut dans une politique ILM active ou inactive doit être conforme.
- Les règles de non-conformité s'appliquent uniquement aux objets dans des compartiments qui n'ont pas le verrouillage d'objets S3 activé ou qui n'ont pas la fonctionnalité de conformité héritée activée.
- Les règles de conformité peuvent s'appliquer aux objets de n'importe quel compartiment ; S3 Object Lock ou la conformité héritée n'ont pas besoin d'être activés pour le compartiment.

"Exemple de politique ILM conforme pour S3 Object Lock"

Exigences pour les compartiments avec S3 Object Lock activé

- Si le paramètre global S3 Object Lock est activé pour le système StorageGRID, vous pouvez utiliser le Tenant Manager, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec S3 Object Lock activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lors de la création du compartiment. Vous ne pouvez pas activer S3 Object Lock pour un compartiment existant.
- Lorsque le verrouillage d'objets S3 est activé pour un compartiment, StorageGRID active automatiquement le versionnage pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage d'objets S3 ni suspendre le versionnage pour ce compartiment.
- Vous pouvez, si vous le souhaitez, spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du Tenant Manager, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui n'ont pas leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors de son chargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage d'objet S3 activé.

Exigences relatives aux objets dans les compartiments avec S3 Object Lock activé

- Pour protéger une version d'objet, vous pouvez définir des paramètres de rétention par défaut pour le compartiment, ou vous pouvez définir des paramètres de rétention pour chaque version d'objet. Les paramètres de rétention au niveau de l'objet peuvent être définis à l'aide de l'application cliente S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent à chaque version d'objet. Une version d'objet peut avoir à la fois une date de conservation et une période de conservation légale, l'une mais pas l'autre, ou aucune. Spécifier une date de conservation ou une période de conservation légale pour un objet protège uniquement la version spécifiée dans la requête. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans les compartiments avec le S3 Object Lock activé

Chaque objet enregistré dans un compartiment avec le verrouillage d'objet S3 activé passe par les étapes suivantes :

1. Ingestion d'objet

Lorsqu'une version d'objet est ajoutée à un compartiment pour lequel le verrouillage d'objet S3 est activé, les paramètres de rétention sont appliqués comme suit :

- Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres au niveau de l'objet sont appliqués. Les paramètres de compartiment par défaut sont ignorés.
- Si aucun paramètre de rétention n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
- Si aucun paramètre de rétention n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par S3 Object Lock.

Si des paramètres de rétention sont appliqués, l'objet et toutes les métadonnées définies par l'utilisateur S3 sont protégés.

2. Conservation et suppression des objets

Plusieurs copies de chaque objet protégé sont stockées par StorageGRID pendant la période de rétention spécifiée. Le nombre et le type exacts de copies d'objet ainsi que les emplacements de stockage sont déterminés par les règles de conformité des politiques ILM actives. La possibilité de supprimer un objet protégé avant que sa date de conservation ne soit atteinte dépend de son mode de rétention.

- Si un objet fait l'objet d'une rétention légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Informations connexes

- ["Créez un compartiment S3"](#)
- ["Mettre à jour la rétention par défaut du verrouillage d'objet S3"](#)
- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Exemple 7 : Stratégie ILM conforme pour S3 Object Lock"](#)

Activer le verrouillage d'objet S3 globalement dans StorageGRID

Si un compte locataire S3 doit se conformer aux exigences réglementaires lors de l'enregistrement de données d'objets, vous devez activer le verrouillage d'objets S3 pour l'ensemble de votre système StorageGRID. L'activation du paramètre global de verrouillage d'objets S3 permet à tout utilisateur locataire S3 de créer et de gérer des compartiments et des objets avec le verrouillage d'objets S3.

Avant de commencer

- Vous avez le ["Autorisation d'accès root"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- `#{post_edited_translations.segment}`
- Vous avez confirmé que la règle par défaut de la stratégie ILM active est conforme. Voir ["Créer une règle ILM par défaut"](#) pour plus de détails.

À propos de cette tâche

Un administrateur de grille doit activer le paramètre global S3 Object Lock pour permettre aux utilisateurs locataires de créer de nouveaux compartiments pour lesquels S3 Object Lock est activé. Une fois ce paramètre activé, il ne peut pas être désactivé.

Examinez les paramètres de conformité des locataires existants après avoir activé le paramètre global S3 Object Lock. Lorsque vous activez ce paramètre, les paramètres S3 Object Lock par locataire dépendent de la version de StorageGRID au moment de la création du locataire.



Le paramètre de conformité global est obsolète. Si vous avez activé ce paramètre dans une version précédente de StorageGRID, le paramètre de verrouillage des objets S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, consultez ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#).

Étapes

1. Sélectionnez **Configuration > Système > Verrouillage d'objet S3**.

`${post_edited_translations.segment}`

2. `${post_edited_translations.segment}`

3. Sélectionnez **Appliquer**.

Une boîte de dialogue de confirmation apparaît et vous rappelle que vous ne pouvez pas désactiver le verrouillage d'objet S3 une fois qu'il est activé.

4. Si vous êtes sûr de vouloir activer définitivement le verrouillage d'objet S3 pour l'ensemble de votre système, sélectionnez **OK**.

`${post_edited_translations.segment}`

- Si la règle par défaut de la stratégie ILM active est conforme, le verrouillage d'objet S3 est désormais activé pour l'ensemble de la grille et ne peut pas être désactivé.
- Si la règle par défaut n'est pas conforme, une erreur s'affiche. Vous devez créer et activer une nouvelle politique ILM qui inclut une règle conforme comme règle par défaut. Sélectionnez **OK**. Ensuite, créez une nouvelle politique, simulez-la et activez-la. Consultez ["Créer une stratégie ILM"](#) pour obtenir des instructions.

Résolvez les erreurs de cohérence lors de la mise à jour de S3 Object Lock ou des paramètres de conformité hérités dans StorageGRID

Si un site de centre de données ou plusieurs nœuds de stockage sur un site deviennent indisponibles, vous devrez peut-être aider les utilisateurs S3 tenant à appliquer des modifications à la configuration S3 Object Lock ou à la configuration Compliance héritée.

Les utilisateurs locataires disposant de compartiments avec S3 Object Lock (ou la conformité héritée) activé peuvent modifier certains paramètres. Par exemple, un utilisateur locataire utilisant S3 Object Lock peut avoir besoin de placer une version d'objet sous séquestre légal.

Lorsqu'un utilisateur locataire met à jour les paramètres d'un compartiment S3 ou la version d'un objet, StorageGRID tente de mettre à jour immédiatement les métadonnées du compartiment ou de l'objet sur l'ensemble de la grille. Si le système ne parvient pas à mettre à jour les métadonnées en raison de l'indisponibilité d'un site de centre de données ou de plusieurs nœuds de stockage, il renvoie une erreur :

```
503: Service Unavailable
```

```
Unable to update compliance settings because the settings can't be  
consistently applied on enough storage services. Contact your grid  
administrator for assistance.
```

Pour résoudre cette erreur, suivez ces étapes :

1. Essayez de rendre tous les nœuds de stockage ou sites à nouveau disponibles dès que possible.
2. Si vous n'êtes pas en mesure de rendre disponibles suffisamment de nœuds de stockage sur chaque site, contactez le support technique, qui peut vous aider à récupérer des nœuds et à garantir que les modifications sont appliquées de manière cohérente sur l'ensemble du grid.
3. Une fois le problème sous-jacent résolu, rappelez à l'utilisateur locataire de réessayer ses modifications de configuration.

Informations connexes

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

`#{post_edited_translations.segment}`

Règles ILM et politique pour la protection et la conservation de base des objets dans StorageGRID

Vous pouvez utiliser les règles et la politique d'exemple suivantes comme point de départ lors de la définition d'une politique ILM pour répondre à vos exigences en matière de protection et de conservation des objets.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

Règle ILM 1 pour l'exemple 1 : copier les données de l'objet sur deux sites

`#{post_edited_translations.segment}`

Définition de la règle	Exemple de valeur
<code>#{post_edited_translations.segment}</code>	<code>#{post_edited_translations.segment}</code>
Nom de la règle	<code>#{post_edited_translations.segment}</code>
Temps de référence	Temps d'ingestion
Placements	<code>#{post_edited_translations.segment}</code>

La section « Analyse des règles » du diagramme de rétention indique :

- La protection contre les pertes de site de StorageGRID s'appliquera pendant toute la durée de cette règle.
- `#{post_edited_translations.segment}`

Reference time ⓘ

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by replicating

1

copies at Site 1

and store objects by replicating

1

copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

StorageGRID site-loss protection will apply for the duration of this rule.

Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

`${post_edited_translations.segment}`

Cet exemple de règle ILM utilise un profil de code d’effacement et un compartiment S3 pour déterminer où et pendant combien de temps l’objet est stocké.

Définition de la règle	Exemple de valeur
Pool de stockage avec plusieurs sites	Un seul pool de stockage réparti sur trois sites (Sites 1, 2, 3) Utilisez le schéma de code d’effacement 6+3
Nom de la règle	<code>\${post_edited_translations.segment}</code>
Temps de référence	Temps d’ingestion
Placements	Pour les objets du compartiment S3 nommé finance-records, créez une copie avec code d’effacement dans le pool spécifié par le profil de code d’effacement. Conservez cette copie indéfiniment.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store forever

Store objects by erasure coding using 6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.



Politique ILM pour l'exemple 1

`${post_edited_translations.segment}`

Une politique ILM typique pour une grille multisite pourrait inclure des règles ILM telles que les suivantes :

- Lors de l'ingestion, stockez tous les objets appartenant au compartiment S3 nommé `finance-records` dans un pool de stockage contenant trois sites. Utilisez le code d'effacement 6+3.
- Si un objet ne correspond pas à la première règle ILM, utilisez la règle ILM par défaut de la stratégie, Two Copies Two Data Centers, pour stocker une copie de cet objet sur le site 1 et une copie sur le site 2.

Proposed policy name
Object Storage Policy

Reason for change
example 1

Manage rules
1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informations connexes

- ["Utilisez les politiques ILM"](#)
- ["Créer des politiques ILM"](#)

Règles ILM et politique pour le filtrage de la taille des objets EC dans StorageGRID

Vous pouvez utiliser les règles et la politique d'exemple suivantes comme points de départ pour définir une politique ILM qui filtre par taille d'objet afin de répondre aux exigences EC recommandées.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`



Le code d'effacement est idéal pour les objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets de moins de 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

Définition de la règle	Exemple de valeur
Nom de la règle	<code>\${post_edited_translations.segment}</code>
Temps de référence	Temps d'ingestion
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
Placements	<code>\${post_edited_translations.segment}</code>

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ×

Object size ▼

greater than ▼

1 ↕

MB ▼ ×

`${post_edited_translations.segment}`

Cet exemple de règle ILM crée deux copies répliquées et ne filtre pas par taille d'objet. Cette règle est la règle par défaut de la stratégie. Comme la première règle exclut tous les objets de plus de 1 Mo, cette règle ne s'applique qu'aux objets de 1 Mo ou moins.

Définition de la règle	Exemple de valeur
Nom de la règle	Deux copies répliquées

Définition de la règle	Exemple de valeur
Temps de référence	Temps d'ingestion
<code>\${post_edited_translations.segment}</code>	Aucune
Placements	<code>\${post_edited_translations.segment}</code>

`${post_edited_translations.segment}`

Cet exemple de politique ILM comprend deux règles ILM :

- La première règle de code d'effacement s'applique à tous les objets supérieurs à 1 Mo.
- La deuxième règle ILM (par défaut) crée deux copies répliquées. Étant donné que les objets de plus de 1 Mo ont été filtrés par la règle 1, la règle 2 ne s'applique qu'aux objets de 1 Mo ou moins.

Règles et politique ILM pour la protection des fichiers image dans StorageGRID

Vous pouvez utiliser les règles et la politique d'exemple suivantes pour garantir que les images supérieures à 1 Mo sont codées par code d'effacement et que deux copies sont réalisées pour les images plus petites.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

`${post_edited_translations.segment}`

Cet exemple de règle ILM utilise un filtrage avancé pour appliquer le code d'effacement à tous les fichiers image de plus de 1 Mo.



Le code d'effacement est idéal pour les objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets de moins de 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

Définition de la règle	Exemple de valeur
Nom de la règle	Fichiers image EC > 1 Mo
Temps de référence	Temps d'ingestion
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
Filtres avancés pour Key	• <code>\${post_edited_translations.segment}</code> • Se termine par .png

Définition de la règle	Exemple de valeur
Placements	<code>\${post_edited_translations.segment}</code>

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and

Key ends with .jpg

or Filter group 2 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and

Key ends with .png

Étant donné que cette règle est configurée comme la première règle de la politique, l'instruction de placement du code d'effacement ne s'applique qu'aux fichiers .jpg et .png de plus de 1 Mo.

`${post_edited_translations.segment}`

Cet exemple de règle ILM utilise le filtrage avancé pour spécifier que les fichiers image de plus petite taille soient répliqués. Étant donné que la première règle de la politique correspond déjà aux fichiers image supérieurs à 1 Mo, cette règle s'applique aux fichiers image de 1 Mo ou moins.

Définition de la règle	Exemple de valeur
Nom de la règle	2 copies pour les fichiers image
Temps de référence	Temps d'ingestion
Filtres avancés pour Key	<code>\${post_edited_translations.segment}</code> - Se termine par .png
Placements	<code>\${post_edited_translations.segment}</code>

Politique ILM pour l'exemple 3 : meilleure protection des fichiers image

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- La deuxième règle crée deux copies de tous les fichiers image restants (c'est-à-dire les images de 1 Mo ou moins).
- `${post_edited_translations.segment}`

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Règles et politiques ILM pour les versions non actuelles des objets S3 dans StorageGRID

Si vous disposez d'un compartiment S3 avec le versionnage activé, vous pouvez gérer les versions d'objets non actuelles en incluant dans votre stratégie ILM des règles qui utilisent « Noncurrent time » comme heure de référence.



Si vous définissez une durée de conservation limitée pour les objets, ces derniers seront définitivement supprimés une fois ce délai écoulé. Assurez-vous de bien comprendre la durée pendant laquelle les objets seront conservés.

Comme le montre cet exemple, vous pouvez contrôler la quantité de stockage utilisée par les objets versionnés en utilisant des instructions de placement différentes pour les versions d'objets non actuelles.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.



Pour effectuer une simulation de politique ILM sur une version non actuelle d'un objet, vous devez connaître l'UUID ou le CBID de cette version d'objet. Pour trouver l'UUID et le CBID, utilisez ["recherche de métadonnées d'objet"](#) tant que l'objet est encore actuel.

Informations connexes

["Comment les objets sont supprimés"](#)

Règle ILM 1 pour l'exemple 4 : Conservez trois copies pendant 10 ans

Cet exemple de règle ILM stocke une copie de chaque objet sur trois sites pendant 10 ans.

Cette règle s'applique à tous les objets, qu'ils soient versionnés ou non.

Définition de la règle	Exemple de valeur
Pools de stockage	Trois pools de stockage, chacun composé de centres de données différents, nommés Site 1, Site 2 et Site 3.

Définition de la règle	Exemple de valeur
Nom de la règle	Trois copies dix ans
Temps de référence	Temps d'ingestion
Placements	Le jour 0, conservez trois copies répliquées pendant 10 ans (3 652 jours), une sur le site 1, une sur le site 2 et une sur le site 3. Au bout de 10 ans, supprimez toutes les copies de l'objet.

Règle ILM 2 pour l'exemple 4 : enregistrez deux copies des versions non actuelles pendant 2 ans

Cette règle ILM d'exemple stocke deux copies des versions non actuelles d'un objet versionné S3 pendant 2 ans.

Étant donné que la règle ILM 1 s'applique à toutes les versions de l'objet, vous devez créer une autre règle pour filtrer les versions non actuelles.

Pour créer une règle qui utilise « Noncurrent time » comme heure de référence, sélectionnez **Oui** à la question « Appliquer cette règle uniquement aux versions antérieures des objets (dans les compartiments S3 avec gestion des versions activée) ? » à l'étape 1 (Saisie des détails) de l'assistant de création d'une règle ILM. Lorsque vous sélectionnez **Oui**, *Noncurrent time* est automatiquement sélectionné comme heure de référence et vous ne pouvez pas en choisir une autre.

1 Enter details

2 Define placements

3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No
☒ Yes

Dans cet exemple, seules deux copies des versions non actuelles sont stockées, et ces copies seront

conservées pendant deux ans.

Définition de la règle	Exemple de valeur
Pools de stockage	Deux pools de stockage, chacun dans un centre de données différent, Site 1 et Site 2.
Nom de la règle	Versions obsolètes : deux exemplaires deux ans
Temps de référence	Temps non actuel Sélectionné automatiquement lorsque vous choisissez Oui à la question « Appliquer cette règle uniquement aux anciennes versions d'objets (dans les compartiments S3 avec le versionnage activé) » dans l'assistant de création d'une règle ILM.
Placements	Le jour 0 par rapport au temps non courant (c'est-à-dire à partir du jour où la version de l'objet devient la version non courante), conservez deux copies répliquées des versions non courantes de l'objet pendant 2 ans (730 jours), une dans le Site 1 et une dans le Site 2. À la fin des 2 ans, supprimez les versions non courantes.

Politique ILM pour l'exemple 4 : objets versionnés S3

Si vous souhaitez gérer les anciennes versions d'un objet différemment de la version actuelle, les règles qui utilisent « Noncurrent time » comme heure de référence doivent apparaître dans la stratégie ILM avant les règles qui s'appliquent à la version actuelle de l'objet.

Une politique ILM pour les objets versionnés S3 peut inclure des règles ILM telles que les suivantes :

- Conservez les versions antérieures (non actuelles) de chaque objet pendant 2 ans, à compter du jour où la version est devenue non actuelle.



Les règles « Noncurrent time » doivent figurer dans la stratégie avant celles qui s'appliquent à la version actuelle de l'objet. Sinon, les versions non actuelles de l'objet ne seront jamais prises en compte par la règle « Noncurrent time ».

- Lors de l'ingestion, créez trois copies répliquées et stockez-en une sur chacun des trois sites. Conservez des copies de la version actuelle de l'objet pendant 10 ans.

Lorsque vous simulez la politique d'exemple, vous vous attendez à ce que les objets de test soient évalués comme suit :

- Toute version non actuelle d'un objet est soumise à la première règle. Si une version non actuelle d'un objet date de plus de deux ans, elle est définitivement supprimée par ILM (toutes les copies de la version non actuelle sont supprimées de la grille).
- La version actuelle de l'objet correspondrait à la deuxième règle. Lorsque la version actuelle de l'objet a été stockée pendant 10 ans, le processus ILM ajoute un marqueur de suppression en tant que 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 associée à la première règle. En conséquence, la copie du site 3 est purgée et les deux copies des sites 1 et 2 sont conservées pendant 2 années supplémentaires.

Règles et politiques ILM pour un comportement d'ingestion strict dans StorageGRID

Vous pouvez utiliser un filtre de localisation et le comportement d'ingestion strict dans une règle pour empêcher l'enregistrement d'objets dans un emplacement de centre de données particulier.

Dans cet exemple, un client basé à Paris ne souhaite pas stocker certains objets hors de l'UE pour des raisons réglementaires. D'autres objets, y compris tous les objets provenant d'autres comptes clients, peuvent être stockés soit dans le centre de données de Paris, soit dans le centre de données des États-Unis.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

Informations connexes

- ["Options d'ingestion"](#)
- ["Créer une règle ILM : Sélectionnez le comportement d'ingestion"](#)

Règle ILM 1 pour l'exemple 5 : Ingestion stricte pour garantir le centre de données de Paris

Cet exemple de règle ILM utilise le comportement d'ingestion Strict pour garantir que les objets enregistrés par un locataire basé à Paris dans des compartiments S3 dont la région est définie sur eu-west-3 (Paris) ne sont jamais stockés dans le centre de données américain.

Cette règle s'applique aux objets appartenant au locataire Paris et dont la région du compartiment S3 est définie sur eu-west-3 (Paris).

Définition de la règle	Exemple de valeur
Compte locataire	Locataire Paris
Filtre avancé	Contrainte de localisation égale à eu-west-3
Pools de stockage	Site 1 (Paris)
Nom de la règle	Ingestion stricte pour garantir le centre de données Paris
Temps de référence	Temps d'ingestion
Placements	Le jour 0, conservez deux copies répliquées indéfiniment dans le site 1 (Paris)
Comportement d'ingestion	Strict. Toujours utiliser les emplacements de cette règle lors de l'ingestion. L'ingestion échoue s'il n'est pas possible de stocker deux copies de l'objet dans le centre de données de Paris.

Strict ingest to guarantee Paris data center

Compliant: Yes
Used in active policy: No
Used in proposed policy: No

Ingest behavior: Strict
Reference time: Ingest time

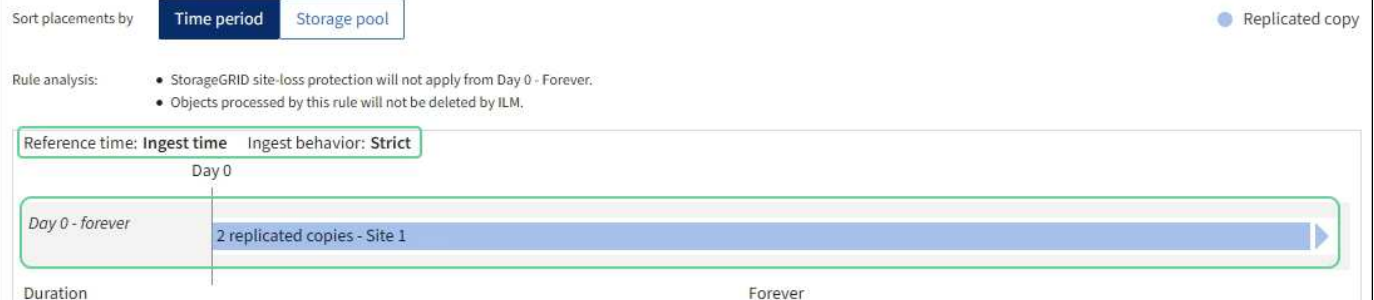
Clone Edit Remove

Filters

This rule applies if:
• Tenant is Paris tenant
And it only applies if objects have this metadata:
• Location constraint is eu-west-3

Time period and placements

Retention diagram Placement instructions



Règle ILM 2 pour l'exemple 5 : Ingestion équilibrée pour les autres objets

Cette règle ILM d'exemple utilise le comportement d'ingestion équilibré pour optimiser l'efficacité ILM des objets non couverts par la première règle. Deux copies de tous les objets correspondant à cette règle seront stockées : une au centre de données US et une au centre de données 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 la règle	Exemple de valeur
Compte locataire	Ignorer
Filtre avancé	Non spécifié
Pools de stockage	Site 1 (Paris) et Site 2 (US)
Nom de la règle	2 copies 2 centres de données
Temps de référence	Temps d'ingestion
Placements	Le jour 0, conservez deux copies répliquées en permanence dans deux centres de données

Définition de la règle	Exemple de valeur
Comportement d'ingestion	Équilibré. Les objets correspondant à cette règle sont placés conformément aux instructions de placement de la règle, si possible. Sinon, des copies provisoires sont créées à n'importe quel emplacement disponible.

Politique ILM pour l'exemple 5 : Combinaison des comportements d'ingestion

La politique ILM d'exemple comprend deux règles qui ont des comportements d'ingestion différents.

Une politique ILM utilisant deux comportements d'ingestion différents peut inclure des règles ILM telles que les suivantes :

- Stockez uniquement dans le centre de données de Paris les objets appartenant au locataire parisien et dont la région du compartiment S3 est définie sur eu-west-3 (Paris). Échouez l'ingestion si le centre de données de Paris est indisponible.
- Stockez tous les autres objets (y compris ceux appartenant au locataire Paris mais ayant une région de compartiment différente) à la fois dans le centre de données américain et dans le centre de données parisien. Créez des copies intermédiaires dans tout emplacement disponible si l'instruction de placement ne peut être satisfaite.

Lorsque vous simulez la politique d'exemple, vous vous attendez à ce que les objets de test soient évalués comme suit :

- Tous les objets appartenant au locataire Paris et dont la région du compartiment S3 est définie sur eu-west-3 correspondent à la première règle et sont stockés dans le centre de données de Paris. Parce que la première règle utilise Strict ingest, ces objets ne sont jamais stockés dans le centre de données américain. Si les Storage Nodes du centre de données de Paris ne sont pas disponibles, l'ingestion échoue.
- Tous les autres objets sont pris en compte par la seconde 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 centre de données. Cependant, comme la seconde règle utilise l'ingestion équilibrée, si un centre de données est indisponible, deux copies intermédiaires sont enregistrées dans tout emplacement disponible.

Comment la modification d'une politique ILM affecte les performances de StorageGRID

Si votre protection des données doit être modifiée ou si vous ajoutez de nouveaux sites, vous pouvez créer et activer une nouvelle politique ILM.

Avant de modifier une politique, vous devez comprendre comment les modifications apportées aux emplacements ILM peuvent temporairement affecter les performances globales d'un système StorageGRID.

Dans cet exemple, un nouveau site StorageGRID a été ajouté lors d'une extension, et une nouvelle stratégie ILM active doit être mise en œuvre pour stocker les données sur ce nouveau site. Pour mettre en œuvre une nouvelle stratégie active, commencez par "[créer une règle](#)". Ensuite, vous devez "[simuler](#)" puis "[activer](#)" la nouvelle stratégie.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

Comment la modification d'une politique ILM affecte les performances

Lorsque vous activez une nouvelle stratégie ILM, les performances de votre système StorageGRID peuvent être temporairement affectées, notamment si les instructions de placement de la nouvelle stratégie nécessitent le déplacement de nombreux objets existants vers de nouveaux emplacements.

Lorsque vous activez une nouvelle stratégie ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Avant d'activer une nouvelle stratégie ILM, vérifiez les modifications apportées à l'emplacement des objets répliqués et à code d'effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lors de l'évaluation et de la mise en œuvre des nouveaux emplacements.

Pour garantir qu'une nouvelle stratégie ILM n'affecte pas le placement des objets répliqués et à code d'effacement existants, vous pouvez ["créer une règle ILM avec un filtre de temps d'ingestion"](#). Par exemple, **Heure d'ingestion est le ou après <date and time>**, afin que la nouvelle règle s'applique uniquement aux objets ingérés à la date et à l'heure spécifiées ou après.

Les types de modifications de stratégie ILM susceptibles d'affecter temporairement les performances de StorageGRID incluent les suivants :

- Application d'un profil de code d'effacement différent aux objets existants codés par effacement.



StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

- Modifier le type de copies requises pour les objets existants, par exemple, convertir un pourcentage important d'objets répliqués en objets à code d'effacement.
- Déplacer des copies d'objets existants vers un emplacement complètement différent ; par exemple, déplacer un grand nombre d'objets vers ou depuis un Cloud Storage Pool ou vers ou depuis un site distant.

Politique ILM active pour l'exemple 6 : protection des données sur deux sites

Dans cet exemple, la politique ILM active a été initialement conçue pour un système StorageGRID à deux sites et utilise deux règles ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

Dans cette politique ILM, les objets appartenant au locataire A sont protégés par code d'effacement 2+1 sur un seul site, tandis que les objets appartenant à tous les autres locataires sont protégés sur deux sites à l'aide d'une réplication à 2 copies.

Règle 1 : code d'effacement sur un seul site pour le locataire A

Définition de la règle	Exemple de valeur
Nom de la règle	Code d'effacement sur un seul site pour le locataire A
Compte locataire	Locataire A
Pool de stockage	Site 1
Placements	code d'effacement 2+1 sur le site 1 depuis le jour 0 et pour toujours

Règle 2 : Réplication sur deux sites pour les autres locataires

Définition de la règle	Exemple de valeur
Nom de la règle	Réplication sur deux sites pour les autres locataires
Compte locataire	Ignorer
Pools de stockage	Site 1 et Site 2
Placements	Deux copies répliquées depuis le jour 0 jusqu'à la fin des temps : une copie sur le site 1 et une copie sur le site 2.

Politique ILM pour l'exemple 6 : Protection des données sur trois sites

Dans cet exemple, la politique ILM est remplacée par une nouvelle politique pour un système StorageGRID à trois sites.

Après avoir étendu le réseau pour ajouter le nouveau site, l'administrateur a créé deux nouveaux pools de stockage : un pool de stockage pour le site 3 et un pool de stockage contenant les trois sites (ce qui n'est pas le même que le pool de stockage par défaut All Storage Nodes). Ensuite, l'administrateur a créé deux nouvelles règles ILM et une nouvelle stratégie ILM, conçue pour protéger les données sur les trois sites.

Lorsque cette nouvelle politique ILM sera activée, les objets appartenant au locataire A seront protégés par code d'effacement 2+1 sur trois sites, tandis que les objets appartenant à d'autres locataires (et les objets plus petits appartenant au locataire A) seront protégés sur trois sites à l'aide d'une réplication à 3 copies.

Règle 1 : code d'effacement à trois sites pour le locataire A

Définition de la règle	Exemple de valeur
Nom de la règle	Codage d'effacement à trois sites pour le locataire A

Définition de la règle	Exemple de valeur
Compte locataire	Locataire A
Pool de stockage	Les 3 sites (y compris le site 1, le site 2 et le site 3)
Placements	code d'effacement 2+1 sur les 3 sites depuis le premier jour et pour toujours

Règle 2 : Réplication sur trois sites pour les autres locataires

Définition de la règle	Exemple de valeur
Nom de la règle	Réplication sur trois sites pour d'autres locataires
Compte locataire	Ignorer
Pools de stockage	Site 1, Site 2 et Site 3
Placements	Trois copies répliquées du jour 0 à l'infini : une copie sur le site 1, une copie sur le site 2 et une copie sur le site 3.

Activation de la stratégie ILM pour l'exemple 6

Lorsque vous activez une nouvelle stratégie ILM, les objets existants peuvent être déplacés vers de nouveaux emplacements ou de nouvelles copies d'objets peuvent être créées pour les objets existants, en fonction des instructions de placement figurant dans les règles nouvelles ou mises à jour.



Des erreurs dans une stratégie ILM peuvent entraîner une perte de données irréversible. Examinez attentivement et simulez la stratégie avant de l'activer afin de confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle stratégie ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Avant d'activer une nouvelle stratégie ILM, vérifiez les modifications apportées à l'emplacement des objets répliqués et à code d'effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lors de l'évaluation et de la mise en œuvre des nouveaux emplacements.

Que se passe-t-il lorsque les instructions de code d'effacement changent

Dans la politique ILM actuellement active pour cet exemple, les objets appartenant au locataire A sont protégés à l'aide du code d'effacement 2+1 sur le site 1. Dans la nouvelle politique ILM, les objets appartenant au locataire A seront protégés à l'aide du code d'effacement 2+1 sur les sites 1, 2 et 3.

Lorsque la nouvelle stratégie ILM est activée, les opérations ILM suivantes se produisent :

- Les nouveaux objets ingérés par le locataire A sont divisés en deux fragments de données et un fragment de parité est ajouté. Ensuite, chacun des trois fragments est stocké sur un site différent.

- Les objets existants appartenant au locataire A sont réévalués lors du processus de numérisation ILM en cours. Parce que les instructions de placement ILM utilisent un nouveau profil de code d'effacement, de tout nouveaux fragments codés par code d'effacement sont créés et répartis sur les trois sites.



Les fragments 2+1 existants sur le site 1 ne sont pas réutilisés. StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

Que se passe-t-il lorsque les instructions de réplication changent

Dans la politique ILM actuellement active pour cet exemple, les objets appartenant à d'autres locataires sont protégés à l'aide de deux copies répliquées dans des pools de stockage sur les sites 1 et 2. Dans la nouvelle politique ILM, les objets appartenant à d'autres locataires seront protégés à l'aide de trois copies répliquées dans des pools de stockage sur les sites 1, 2 et 3.

Lorsque la nouvelle stratégie ILM est activée, les opérations ILM suivantes se produisent :

- Lorsqu'un locataire autre que le locataire A ingère un nouvel objet, StorageGRID crée trois copies et enregistre une sur chaque site.
- Les objets existants appartenant à ces autres locataires sont réévalués lors du processus d'analyse ILM en cours. Parce que les copies d'objets existantes sur Site 1 et Site 2 continuent de satisfaire aux exigences de réplication de la nouvelle règle ILM, StorageGRID n'a besoin de créer qu'une seule nouvelle copie de l'objet pour Site 3.

Impact de l'activation de cette politique sur les performances

Lorsque la stratégie ILM de cet exemple est activée, les performances globales de ce système StorageGRID seront temporairement affectées. Des ressources de grille supérieures à la normale seront nécessaires pour créer de nouveaux fragments à code d'effacement pour les objets existants du locataire A et de nouvelles copies répliquées sur le site 3 pour les objets existants des autres locataires.

Suite à la modification de la politique ILM, les requêtes de lecture et d'écriture des clients pourraient temporairement subir des latences supérieures à la normale. Les latences reviendront à des niveaux normaux une fois que les instructions de placement auront été entièrement appliquées sur l'ensemble de la grille.

Pour éviter les problèmes de ressources lors de l'activation d'une nouvelle stratégie ILM, vous pouvez utiliser le filtre avancé Ingest time dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez Ingest time sur une valeur supérieure ou égale à l'heure approximative à laquelle la nouvelle stratégie entrera en vigueur afin de garantir que les objets existants ne soient pas déplacés inutilement.



Contactez le support technique si vous devez ralentir ou augmenter la vitesse à laquelle les objets sont traités après une modification de la stratégie ILM.

Stratégie ILM conforme pour S3 Object Lock dans StorageGRID

Vous pouvez utiliser le compartiment S3, les règles ILM et la stratégie ILM de cet exemple comme point de départ lors de la définition d'une stratégie ILM pour répondre aux exigences de protection et de conservation des objets dans les compartiments avec S3 Object Lock activé.



Si vous avez utilisé l'ancienne fonctionnalité de conformité dans les versions précédentes de StorageGRID, vous pouvez également utiliser cet exemple pour gérer les compartiments existants sur lesquels l'ancienne fonctionnalité de conformité est activée.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte.

Informations connexes

- ["Gérez les objets avec S3 Object Lock"](#)
- ["Créer une politique ILM"](#)

Compartiment et objets pour l'exemple de S3 Object Lock

Dans cet exemple, un compte locataire S3 nommé Bank of ABC a utilisé le Tenant Manager pour créer un compartiment avec le S3 Object Lock activé afin de stocker des enregistrements bancaires critiques.

Définition du compartiment	Exemple de valeur
Nom du compte locataire	Banque ABC
Nom du compartiment	relevés bancaires
Région du compartiment	us-east-1 (par défaut)

Chaque objet et chaque version d'objet ajoutés au compartiment bank-records utiliseront les valeurs suivantes pour les paramètres `retain-until-date` et `legal hold`.

Paramétrage pour chaque objet	Exemple de valeur
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 décembre 2030) Chaque version d'objet possède son propre <code>retain-until-date</code> paramètre. Ce paramètre peut être augmenté, mais pas diminué.
<code>legal hold</code>	« OFF » (Sans effet) Une restriction légale peut être appliquée ou levée à toute version d'un objet à tout moment pendant sa période de conservation. Si un objet fait l'objet d'une restriction légale, il ne peut être supprimé même si la <code>retain-until-date</code> a été atteinte.

Exemple de règle ILM 1 pour S3 Object Lock : profil de code d'effacement avec correspondance de compartiment

Cette règle ILM s'applique uniquement au compte locataire S3 nommé Bank of ABC. Elle identifie tout objet dans le `bank-records` compartiment et utilise ensuite le code d'effacement pour stocker l'objet sur des nœuds de stockage répartis sur trois sites de centres de données, en utilisant un profil de code d'effacement 6+3. Cette règle répond aux exigences des compartiments avec S3 Object Lock activé : une copie est conservée sur les nœuds de stockage du jour 0 à toujours, en utilisant la date d'ingestion comme référence.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle conforme : Objets EC dans le compartiment bank-records - Bank of ABC
Compte locataire	Banque ABC
Nom du compartiment	bank-records
Filtre avancé	Taille de l'objet (Mo) supérieure à 1 Remarque : Ce filtre garantit que le code d'effacement n'est pas utilisé pour les objets de 1 Mo ou moins.

Définition de la règle	Exemple de valeur
Temps de référence	Temps d'ingestion
Placements	Dès le premier jour, stockez pour toujours
Profil de code d'effacement	• Créez une copie à code d'effacement sur les nœuds de stockage de trois sites de centres de données • Utilisez un schéma de code d'effacement 6+3

Règle ILM 2 pour l'exemple de S3 Object Lock : règle non conforme

Cet exemple de règle ILM stocke initialement deux copies répliquées d'objet sur des Storage Nodes. Après un an, elle stocke une copie dans un Cloud Storage Pool de façon permanente. Parce que cette règle utilise un Cloud Storage Pool, elle n'est pas conforme et ne s'appliquera pas aux objets dans des compartiments avec S3 Object Lock activé.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle non conforme : Utiliser un Cloud Storage Pool
Comptes de locataire	Non spécifié
Nom du compartiment	Non spécifié, mais ne s'appliquera qu'aux compartiments qui n'ont pas le verrouillage d'objets S3 (ou l'ancienne fonctionnalité de conformité) activé.
Filtre avancé	Non spécifié

Définition de la règle	Exemple de valeur
Temps de référence	Temps d'ingestion

Définition de la règle	Exemple de valeur
Placements	- Le jour 0, conservez deux copies répliquées sur les nœuds de stockage dans Data Center 1 et Data Center 2 pendant 365 jours - Après un an, conservez une copie répliquée dans un Cloud Storage Pool pour toujours

Règle ILM 3 pour l'exemple de S3 Object Lock : règle par défaut

Cette règle ILM d'exemple copie les données d'objet vers des pools de stockage dans deux centres de données. Cette règle conforme est conçue pour être la règle par défaut de la stratégie ILM. Elle ne comporte aucun filtre, n'utilise pas l'heure de référence Noncurrent et satisfait aux exigences des compartiments avec S3 Object Lock activé : deux copies d'objet sont conservées sur les Storage Nodes du jour 0 à toujours, en utilisant Ingest comme heure de référence.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle de conformité par défaut : Deux copies deux centres de données
Compte locataire	Non spécifié
Nom du compartiment	Non spécifié
Filtre avancé	Non spécifié

Définition de la règle	Exemple de valeur
Temps de référence	Temps d'ingestion
Placements	Depuis le jour 0 et pour toujours, conservez deux copies répliquées : une sur les nœuds de stockage dans Data Center 1 et une sur les nœuds de stockage dans Data Center 2.

Exemple de politique ILM conforme pour S3 Object Lock

Pour créer une stratégie ILM qui protège efficacement tous les objets de votre système, y compris ceux des compartiments avec S3 Object Lock activé, vous devez sélectionner des règles ILM qui répondent aux exigences de stockage de tous les objets. Ensuite, vous devez simuler et activer la stratégie.

Ajouter des règles à la politique

Dans cet exemple, la politique ILM comprend trois règles ILM, dans l'ordre suivant :

1. Une règle conforme qui utilise le code d'effacement pour protéger les objets de plus de 1 Mo dans un compartiment spécifique avec S3 Object Lock activé. Les objets sont stockés sur les Storage Nodes du jour 0 à toujours.
2. Une règle non conforme qui crée deux copies d'objet répliquées sur les Storage Nodes pendant un an, puis déplace définitivement une copie d'objet vers un Cloud Storage Pool. Cette règle ne s'applique pas aux compartiments avec S3 Object Lock activé, car elle utilise un Cloud Storage Pool.

3. La règle de conformité par défaut qui crée deux copies d'objets répliquées sur les Storage Nodes, du jour 0 pour toujours.

Simuler la règle

Après avoir ajouté des règles à votre stratégie, choisi une règle conforme par défaut et organisé les autres règles, vous devez simuler la stratégie en testant des objets provenant du compartiment avec S3 Object Lock activé et d'autres compartiments. Par exemple, lorsque vous simulez la stratégie d'exemple, vous pouvez vous attendre à ce que les objets de test soient évalués comme suit :

- La première règle ne correspondra qu'aux objets de test supérieurs à 1 Mo dans le compartiment bank-records du locataire Bank of ABC.
- La deuxième règle s'appliquera à tous les objets dans tous les compartiments non conformes pour tous les autres comptes locataires.
- La règle par défaut correspondra à ces objets :
 - Objets de 1 Mo ou moins dans le compartiment bank-records pour le locataire Bank of ABC.
 - Objets dans tout autre compartiment pour lequel le verrouillage d'objets S3 est activé pour tous les autres comptes locataires.

Activez la règle

Lorsque vous êtes pleinement convaincu que la nouvelle politique protège les données d'objet comme prévu, vous pouvez l'activer.

Comment le cycle de vie des compartiments S3 et la politique ILM interagissent dans StorageGRID

Selon votre configuration de cycle de vie, les objets suivent les paramètres de rétention soit du cycle de vie du compartiment S3, soit d'une politique ILM.

Exemple de priorité donnée au cycle de vie des compartiments par rapport à la politique ILM

Règle ILM

- Règle basée sur une référence temporelle non actuelle : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence à l'heure d'ingestion (par défaut) : le jour 0, conserver X copies pendant 50 jours

Cycle de vie du bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Il correspond au filtre de cycle de vie du compartiment avec le préfixe « docs/ ».
 - Au bout de 100 jours, un marqueur de suppression est créé et « docs/text » devient non actuel.
 - Après 5 jours, soit un total de 105 jours depuis l'ingestion, « docs/text » est supprimé.
 - Après 95 jours, soit un total de 200 jours depuis l'ingest et 100 jours depuis la création du delete-marker, le delete-marker expiré est supprimé.
- Un objet nommé « video/movie » est ingéré. Il ne correspond pas au filtre et utilise la politique de rétention ILM.

- Au bout de 50 jours, un marqueur de suppression est créé et "video/movie" devient non actuel.
- Après 20 jours, soit un total de 70 jours depuis l'ingestion, « vidéo/film » est supprimé.
- Après 30 jours, soit un total de 100 jours depuis l'ingestion et 50 jours depuis la création du marqueur de suppression, le marqueur de suppression expiré est supprimé.

Exemple de cycle de vie d'un seau avec conservation implicite illimitée

Règle ILM

- Règle basée sur une référence temporelle non actuelle : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence à l'heure d'ingestion (par défaut) : le jour 0, conserver X copies pendant 50 jours

Cycle de vie du bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker": true}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Il correspond au filtre de cycle de vie du compartiment avec le préfixe « docs/ ».

L'`Expiration` action s'applique uniquement aux marqueurs de suppression expirés, ce qui implique de conserver tout le reste indéfiniment (à partir de « docs/ »).

Les marqueurs de suppression commençant par « docs/ » sont supprimés lorsqu'ils expirent.

- Un objet nommé « video/movie » est ingéré. Il ne correspond pas au filtre et utilise la politique de rétention ILM.
 - Au bout de 50 jours, un marqueur de suppression est créé et "video/movie" devient non actuel.
 - Après 20 jours, soit un total de 70 jours depuis l'ingestion, « vidéo/film » est supprimé.
 - Après 30 jours, soit un total de 100 jours depuis l'ingestion et 50 jours depuis la création du marqueur de suppression, le marqueur de suppression expiré est supprimé.

Exemple d'utilisation du cycle de vie des compartiments pour dupliquer l'ILM et nettoyer les marqueurs de suppression expirés

Règle ILM

- Règle basée sur une référence temporelle non actuelle : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence à l'heure d'ingestion (par défaut) : au jour 0, conserver X copies indéfiniment

Cycle de vie du bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Résultat

- La politique ILM est dupliquée dans le cycle de vie du bucket.
 - La règle de conservation permanente de la stratégie ILM est conçue pour supprimer manuellement les objets et nettoyer les versions non actuelles après 20 jours. Par conséquent, la règle de durée d'ingestion conservera indéfiniment les marqueurs de suppression expirés.

- Le cycle de vie du compartiment reproduit le comportement de la politique ILM tout en ajoutant `"ExpiredObjectDeleteMarker": true`, ce qui supprime les marqueurs de suppression une fois qu'ils ont expiré
- Un objet est ingéré. L'absence de filtre signifie que le cycle de vie du compartiment s'applique à tous les objets et remplace les paramètres de rétention ILM.
 - Lorsqu'un locataire soumet une demande de suppression d'objet, un marqueur de suppression est créé et l'objet devient non actuel.
 - Au bout de 20 jours, l'objet obsolète est supprimé et l'indicateur de suppression devient expiré.
 - Peu après, le marqueur de suppression expiré est supprimé.

Renforcement du système pour StorageGRID

Découvrez le renforcement du système pour StorageGRID

Le renforcement du système est le processus visant à éliminer autant de risques de sécurité que possible d'un système StorageGRID.

Lors de l'installation et de la configuration de StorageGRID, utilisez ces instructions pour vous aider à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité.

Vous devriez déjà appliquer les meilleures pratiques du secteur en matière de renforcement de la sécurité des systèmes. Par exemple, vous utilisez des mots de passe robustes pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur des certificats lorsque cela est possible. Ces meilleures pratiques doivent inclure des mesures de sécurité physique et environnementale qui limitent l'accès physique ainsi que la protection du centre de données physique et de l'infrastructure de support. Vous devez également vous référer à toute norme et recommandation réglementaire applicable à votre entreprise et à votre zone géographique.

StorageGRID suit la procédure ["Politique de gestion des vulnérabilités NetApp"](#). Les vulnérabilités signalées sont vérifiées et traitées conformément au processus de réponse aux incidents de sécurité des produits.

Lors du renforcement de la sécurité d'un système StorageGRID, tenez compte des points suivants :

- Lequel des trois réseaux StorageGRID avez-vous implémenté ? Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau Admin, le réseau Client, ou les deux. Chaque réseau présente des considérations de sécurité différentes.
- **Le type de plateformes** que vous utilisez pour les différents nœuds de votre système StorageGRID. Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, dans un moteur de conteneurs sur des hôtes Linux, ou sous forme d'appliances matérielles dédiées. Chaque type de plateforme possède ses propres bonnes pratiques de sécurisation.
- **Degré de confiance des comptes locataires.** Si vous êtes un fournisseur de services utilisant des comptes locataires non fiables, vos préoccupations en matière de sécurité différeront de celles liées à l'utilisation exclusive de comptes locataires internes de confiance.
- **Quelles exigences et conventions de sécurité** votre organisation suit. Vous pourriez devoir respecter des exigences réglementaires ou internes spécifiques.

Recommandations de renforcement pour les mises à niveau logicielles StorageGRID

Vous devez maintenir votre système StorageGRID et les services associés à jour afin de 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 majeure la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire la durée pendant laquelle les vulnérabilités connues sont actives et de réduire la surface globale d'attaque. De plus, les versions les plus récentes de StorageGRID contiennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions antérieures.

Consultez l' "[Outil NetApp Interoperability Matrix Tool](#)" IMT pour déterminer quelle version du logiciel StorageGRID vous devez utiliser. Lorsqu'un correctif est requis, NetApp donne la priorité à la création de mises à jour pour les versions les plus récentes. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs les plus récents de StorageGRID, rendez-vous sur "[NetApp Téléchargements : StorageGRID](#)".
- Pour mettre à niveau le logiciel StorageGRID, consultez le "[instructions de mise à niveau](#)".
- Pour appliquer un correctif, consultez le "[Procédure de correctif StorageGRID](#)".

Mises à niveau des services externes

Les services externes peuvent présenter des vulnérabilités qui affectent StorageGRID indirectement. Assurez-vous que les services dont dépend StorageGRID sont maintenus à jour. Ces services incluent LDAP, KMS (ou serveur KMIP), DNS et NTP.

Pour obtenir la liste des versions prises en charge, consultez la "[Outil NetApp Interoperability Matrix Tool](#)".

Mises à niveau des hyperviseurs

Si vos nœuds StorageGRID fonctionnent sous VMware ou un autre hyperviseur, vous devez vous assurer que le logiciel de l'hyperviseur et le firmware sont à jour.

Pour obtenir la liste des versions prises en charge, consultez la "[Outil NetApp Interoperability Matrix Tool](#)".

Mises à niveau des nœuds Linux

Si vos nœuds StorageGRID utilisent des plateformes hôtes Linux, vous devez vous assurer que les mises à jour de sécurité et les mises à jour du noyau sont appliquées au système d'exploitation hôte. De plus, vous devez appliquer les mises à jour du firmware au matériel vulnérable dès que ces mises à jour sont disponibles.

Pour obtenir la liste des versions prises en charge, consultez la "[Outil NetApp Interoperability Matrix Tool](#)".

Recommandations de renforcement pour les réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud de grille, ce qui vous permet de configurer le réseau de chaque nœud de grille individuellement afin de répondre à vos exigences de sécurité et d'accès.

Pour des informations détaillées sur les réseaux StorageGRID, consultez le ["Types de réseaux StorageGRID"](#).

Lignes directrices pour le réseau Grid

Vous devez configurer un réseau Grid pour tout le trafic interne de StorageGRID. Tous les nœuds du réseau Grid sont sur le réseau Grid et doivent pouvoir communiquer avec tous les autres nœuds.

Lors de la configuration du réseau Grid, suivez ces instructions :

- Assurez-vous que le réseau est protégé contre les clients non fiables, tels que ceux présents sur l'internet ouvert.
- Dans la mesure du possible, utilisez le réseau Grid exclusivement pour le trafic interne. Les réseaux Admin et Client disposent de restrictions de pare-feu supplémentaires qui bloquent le trafic externe vers les services internes. L'utilisation du réseau Grid pour le trafic client externe est prise en charge, mais cette utilisation offre moins de couches de protection.
- Si le déploiement StorageGRID s'étend sur plusieurs centres de données, utilisez un réseau privé virtuel (VPN) ou un équivalent sur le réseau Grid pour assurer une protection supplémentaire du trafic interne.
- Certaines procédures de maintenance nécessitent un accès Secure Shell (SSH) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds du grid. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients de confiance.

Directives pour le réseau d'administration

Le réseau d'administration est généralement utilisé pour les tâches administratives (par des employés autorisés utilisant Grid Manager ou SSH) et pour communiquer avec d'autres services de confiance tels que LDAP, DNS, NTP ou KMS (ou serveur KMIP). Cependant, StorageGRID n'impose pas cette utilisation en interne.

Si vous utilisez le réseau d'administration, suivez ces instructions :

- Bloquez tous les ports de trafic interne sur le réseau d'administration. Voir le ["liste des ports internes"](#).
- Si des clients non fiables peuvent accéder au réseau d'administration, bloquez l'accès à StorageGRID sur le réseau d'administration à l'aide d'un pare-feu externe.

Lignes directrices pour le réseau client

Le réseau client est généralement utilisé par les locataires et pour communiquer avec des services externes, tels que le service de réplication CloudMirror ou un autre service de la plateforme. Cependant, StorageGRID n'impose pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez ces directives :

- Bloquez tous les ports de trafic interne sur le réseau client. Voir le ["liste des ports internes"](#).
- N'acceptez le trafic client entrant que sur les points de terminaison explicitement configurés. Consultez les informations à propos de ["gestion des contrôles de pare-feu"](#).

Recommandations 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 sous forme d'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud possède ses

propres bonnes pratiques de sécurisation.

Contrôlez l'accès IPMI distant au BMC

Vous pouvez activer ou désactiver l'accès IPMI distant pour tous les équipements contenant un BMC. L'interface IPMI distante permet à toute personne disposant d'un compte BMC et d'un mot de passe d'accéder au matériel de bas niveau de vos équipements StorageGRID. Si vous n'avez pas besoin d'un accès IPMI distant au BMC, désactivez cette option.

- Pour contrôler l'accès IPMI à distance au BMC dans Grid Manager, allez dans **Configuration > Sécurité > Paramètres de sécurité > Appareils** :
 - Décochez la case **Activer l'accès IPMI à distance** pour désactiver l'accès IPMI au BMC.
 - Sélectionnez la case à cocher **Activer l'accès IPMI à distance** pour activer l'accès IPMI au BMC.

Pour plus d'informations sur le renforcement de la sécurité de BMC, consultez la "[Renforcez les Baseboard Management Controllers](#)" fiche d'information sur la cybersécurité de la "[National Security Agency \(NSA\)](#)" et la "[Agence de cybersécurité et de sécurité des infrastructures \(CISA\)](#)".

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez examiner les configurations des pare-feu externes et les modifier afin que le trafic ne soit accepté qu'à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Vous devez "[gérer les contrôles du pare-feu interne](#)" pour empêcher l'accès réseau sur tous les ports, à l'exception de ceux nécessaires au déploiement spécifique de votre grille. Les modifications de configuration que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Plus précisément, vous pouvez gérer les domaines suivants :

- **Adresses privilégiées** : Vous pouvez autoriser certaines adresses IP ou certains sous-réseaux à accéder à des ports fermés par les paramètres de l'onglet Manage external access.
- **Gérer l'accès externe** : Vous pouvez fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non fiable** : Vous pouvez spécifier si un nœud fait confiance au trafic entrant provenant du réseau client, ainsi que les ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non fiable est configuré.

Bien que ce pare-feu interne offre une couche de protection supplémentaire 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, consultez "[Ports internes de StorageGRID](#)" et "[Ports utilisés pour les communications externes](#)".

Désactivez les services inutilisés

Pour tous les nœuds StorageGRID, vous devez désactiver ou bloquer l'accès aux services inutilisés. Par exemple, si vous ne prévoyez pas d'utiliser DHCP, utilisez le Grid Manager pour fermer le port 68. Sélectionnez **Configuration > Contrôle du pare-feu > Gérer l'accès externe**. Ensuite, modifiez le statut du port 68 de **Ouvert** à **Fermé**.

Virtualisation, conteneurs et matériel partagé

Pour tous les nœuds StorageGRID, évitez d'exécuter StorageGRID sur le même matériel physique que des logiciels non fiables. Ne supposez pas que les protections de l'hyperviseur empêcheront les logiciels malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le logiciel malveillant existent sur le même matériel physique. Par exemple, les attaques Meltdown et Spectre exploitent des vulnérabilités critiques dans les processeurs modernes et permettent à des programmes de voler des données en mémoire sur le même ordinateur.

Protégez les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID via le réseau pendant leur installation. Les nœuds ne sont pas entièrement sécurisés tant qu'ils n'ont pas rejoint la grille.

Limiter l'accès physique au matériel

Vous devez limiter l'accès physique aux nœuds des appliances matérielles StorageGRID, ainsi qu'aux hôtes de machines virtuelles VMware et aux hôtes Linux exécutant StorageGRID, aux seuls administrateurs autorisés. Quelques exemples de contrôles d'accès physique incluent les serrures, les agents de sécurité, les barrières physiques et la vidéosurveillance.

Les nœuds matériels sont conçus pour être installés et utilisés uniquement par des administrateurs autorisés. N'autorisez pas les administrateurs non autorisés à accéder aux nœuds matériels.

Directives pour les nœuds d'administration

Les nœuds d'administration fournissent des services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez au Grid Manager ou au Tenant Manager, vous vous connectez à un nœud d'administration.

Suivez ces instructions pour sécuriser les nœuds d'administration de votre système StorageGRID :

- Sécurisez tous les nœuds d'administration contre les clients non fiables, notamment ceux situés sur Internet. Assurez-vous qu'aucun client non fiable ne puisse 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. Attribuez à chaque groupe d'utilisateurs les autorisations minimales requises pour leur rôle et utilisez le mode d'accès en lecture seule pour empêcher les utilisateurs de modifier la configuration.
- Lorsque vous utilisez des points de terminaison d'équilibrage de charge StorageGRID, utilisez des nœuds de passerelle au lieu de nœuds d'administration pour le trafic client non fiable.
- Si vous avez des locataires non fiables, ne leur accordez pas d'accès direct au Tenant Manager ni à l'API de gestion des locataires. À la place, demandez à ces locataires non fiables d'utiliser un portail locataire ou un système de gestion des locataires externe, qui interagit avec l'API de gestion des locataires.
- Vous pouvez également utiliser un proxy d'administration pour un meilleur contrôle des communications AutoSupport des nœuds d'administration vers le support NetApp. Consultez la procédure pour ["création d'un proxy d'administration"](#).
- Vous pouvez utiliser les ports restreints 8443 et 9443 pour séparer les communications entre Grid Manager et Tenant Manager. Bloquez le port partagé 443 et limitez les requêtes des locataires au port 9443 pour une protection supplémentaire.
- Vous pouvez également utiliser des nœuds d'administration distincts pour les administrateurs de grille et les utilisateurs locataires.

Pour plus d'informations, consultez les instructions pour ["administration de StorageGRID"](#).

Directives relatives aux nœuds de stockage

Les nœuds de stockage gèrent et stockent les données et métadonnées des objets. Suivez ces instructions pour sécuriser les nœuds de stockage de votre système StorageGRID.

- N'autorisez pas les clients non fiables à se connecter directement aux nœuds de stockage. Utilisez un point de terminaison d'équilibrage de charge fourni par un nœud de passerelle ou un équilibreur de charge tiers.
- N'activez pas les services sortants pour les locataires non approuvés. Par exemple, lors de la création du compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser sa propre source d'identité et n'autorisez pas l'utilisation des services de la plateforme. Consultez la procédure pour ["création d'un compte locataire"](#).
- Utilisez un répartiteur de charge tiers pour le trafic des clients non fiables. L'équilibrage de charge tiers offre un meilleur contrôle et des niveaux de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour un contrôle accru des Cloud Storage Pools et des communications des services de plateforme des nœuds de stockage vers les services externes. Consultez les étapes pour ["création d'un proxy de stockage"](#).
- Vous pouvez éventuellement vous connecter à des services externes via le Client Network. Ensuite, sélectionnez **Configuration > Security > Firewall control > Untrusted Client Networks** et indiquez que le Client Network sur le Storage Node n'est pas approuvé. Le Storage Node n'accepte plus aucun trafic entrant sur le Client Network, mais continue d'autoriser les requêtes sortantes pour les Platform Services.

Directives pour les nœuds de passerelle

Les nœuds de passerelle offrent une interface d'équilibrage de charge optionnelle permettant aux applications clientes de se connecter à StorageGRID. Suivez ces instructions pour sécuriser les nœuds de passerelle de votre système StorageGRID :

- Configurez et utilisez les points de terminaison de l'équilibreur de charge. Voir ["Considérations relatives à l'équilibrage de charge"](#).
- Utilisez un équilibreur de charge tiers entre le client et le nœud de passerelle ou les nœuds de stockage pour le trafic client non fiable. L'équilibrage de charge tiers offre un meilleur contrôle et une protection renforcée contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut toujours être configuré pour transiter par un point de terminaison d'équilibrage de charge interne ou être envoyé directement aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, vous pouvez éventuellement faire en sorte que les clients se connectent via le réseau client. Ensuite, sélectionnez **Configuration > Sécurité > Contrôle du pare-feu > Réseaux clients non approuvés** et indiquez que le réseau client sur le nœud passerelle n'est pas approuvé. Le nœud passerelle n'accepte le trafic entrant que sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge.

Directives relatives aux nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour être utilisées dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. D'autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds passerelle. Vous pouvez combiner des nœuds appliances avec des nœuds logiciels ou déployer des grilles entièrement composées d'appliances.

Suivez ces instructions pour sécuriser les nœuds matériels de votre système StorageGRID :

- Si l'apppliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non fiables d'accéder à SANtricity System Manager via le réseau.
- Si l'appareil est équipé d'un contrôleur de gestion de carte mère (BMC), sachez que le port de gestion du BMC permet un accès matériel de bas niveau. Connectez le port de gestion du BMC uniquement à un réseau de gestion interne sécurisé et de confiance.

Vous pouvez établir un VLAN pour isoler les connexions réseau BMC et restreindre l'accès Internet du BMC aux réseaux de confiance. Pour plus d'informations sur l'application de la séparation par VLAN, consultez la "[Renforcez les Baseboard Management Controllers](#)" fiche d'information sur la cybersécurité de la "[National Security Agency \(NSA\)](#)" et de la "[Agence de cybersécurité et de sécurité des infrastructures \(CISA\)](#)".

Si aucun réseau de gestion interne sécurisé et fiable n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué. Le support technique pourrait demander un accès temporaire lors d'une demande d'assistance.

- Si l'appareil prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme Intelligent Platform Management Interface (IPMI), bloquez le trafic non fiable sur le port 623.



Vous pouvez activer ou désactiver l'accès IPMI distant pour tous les équipements contenant un BMC. L'interface IPMI distante permet à toute personne disposant d'un compte et d'un mot de passe BMC d'accéder au matériel de bas niveau de vos équipements StorageGRID. Si vous n'avez pas besoin d'un accès IPMI distant au BMC, désactivez cette option en utilisant l'une des méthodes suivantes : + Dans Grid Manager, accédez à **Configuration > Sécurité > Paramètres de sécurité > Équipements** et décochez la case **Activer l'accès IPMI distant**. + Dans l'API de gestion Grid, utilisez le point de terminaison privé : PUT /private/bmc.

+ Vous pouvez aussi [désactiver l'accès IPMI à distance](#).

- Pour les modèles d'appiances contenant des disques SED, FDE ou FIPS NL-SAS que vous gérez avec SANtricity System Manager, "[activer et configurer SANtricity Drive Security](#)".
- Pour les modèles d'appiances contenant des SSD NVMe SED ou FIPS que vous gérez à l'aide de StorageGRID Appliance Installer et de Grid Manager, "[activer et configurer le chiffrement des disques StorageGRID](#)".
- Pour les appareils sans disques SED, FDE ou FIPS, utilisez un serveur de gestion de clés (KMS) pour "[activer et configurer le chiffrement du nœud logiciel StorageGRID](#)".

Informations connexes

["Découvrez la sécurité des disques dans SANtricity System Manager"](#)

Recommandations de renforcement pour TLS et SSH dans StorageGRID

Vous devez contrôler l'accès SSH, remplacer les certificats TLS par défaut et sélectionner la politique de sécurité appropriée pour les connexions TLS et SSH.

Directives de renforcement pour les certificats

Vous devez remplacer les certificats par défaut créés lors de l'installation par vos propres certificats personnalisés.

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès web à StorageGRID n'est pas conforme à leurs politiques de sécurité informatique. 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 devriez 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 de gestion du Grid et à l'API de gestion du Tenant.
- **Certificat API S3** : Utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications clientes S3 utilisent pour charger et télécharger des données d'objet.

Voir ["Gérer les certificats de sécurité"](#) pour plus de détails et d'instructions.



StorageGRID gère séparément les certificats utilisés pour les points de terminaison de l'équilibreur de charge. Pour configurer les certificats de l'équilibreur de charge, consultez ["Configurer les points de terminaison de l'équilibreur de charge"](#).

Lorsque vous utilisez des certificats de serveur personnalisés, suivez ces instructions :

- Les certificats doivent avoir un *subjectAltName* correspondant aux entrées DNS de StorageGRID. Pour plus de détails, consultez la section 4.2.1.6, « Subject Alternative Name », dans ["RFC 5280 : Profil de certificat et de liste de révocation de certificats PKIX"](#).
- Dans la mesure du possible, évitez l'utilisation de certificats génériques. Une exception à cette règle concerne le certificat d'un endpoint S3 de type hébergement virtuel, qui requiert l'utilisation d'un caractère générique si les noms de buckets ne sont pas connus à l'avance.
- Lorsque vous devez utiliser des caractères génériques dans les certificats, vous devez prendre des mesures supplémentaires pour réduire les risques. Utilisez un modèle de caractère générique tel que `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour d'autres applications. Ce modèle fonctionne également avec l'accès S3 par chemin, tel que `dc1-s1.s3.example.com/mybucket`.
- Définissez des durées d'expiration courtes pour les certificats (par exemple, 2 mois) et utilisez l'API de gestion de la grille pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

De plus, les clients doivent utiliser une vérification stricte du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement pour la politique TLS et SSH

Vous pouvez sélectionner une politique de sécurité pour déterminer les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées aux services internes StorageGRID.

La politique de sécurité contrôle la façon dont TLS et SSH chiffrent les données en transit. En tant que bonne pratique, vous devez désactiver les options de chiffrement qui ne sont pas requises pour la compatibilité des applications. Utilisez la politique Moderne par défaut, sauf si votre système doit être conforme aux Common Criteria, à la norme FIPS 140-2, ou si vous devez utiliser d'autres algorithmes de chiffrement.

Voir ["Gérez la politique TLS et SSH"](#) pour plus de détails et d'instructions.

Gérer l'accès SSH externe

Pour renforcer la sécurité du système, l'accès SSH externe est bloqué par défaut. N'activez l'accès SSH que lorsque vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage. Consultez

["Gérer l'accès SSH externe"](#) pour plus de détails et d'instructions.

Recommandations de renforcement pour les journaux, les mots de passe et les messages d'audit dans StorageGRID

En plus de suivre les directives de renforcement de la sécurité pour les réseaux et les nœuds StorageGRID, vous devez également suivre les directives de renforcement de la sécurité pour les autres zones du système StorageGRID.

Mot de passe d'installation temporaire

Pour sécuriser le système StorageGRID lors de l'installation, définissez un mot de passe sur la page de mot de passe temporaire de l'installateur dans l'interface utilisateur d'installation de StorageGRID ou dans l'API d'installation. Une fois défini, ce mot de passe s'applique à toutes les méthodes d'installation de StorageGRID, y compris l'interface utilisateur, l'API d'installation et le script `configure-storagegrid.py`.

Pour plus d'informations, consultez :

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

Journaux et messages d'audit

Protégez toujours les journaux et la sortie des messages d'audit StorageGRID de manière sécurisée. Les journaux et les messages d'audit StorageGRID fournissent des informations inestimables du point de vue du support et de la disponibilité du système. De plus, les informations et les détails contenus dans les journaux et la sortie des messages d'audit StorageGRID sont généralement de nature sensible.

Configurez StorageGRID pour envoyer les événements de sécurité à un serveur syslog externe. Si vous utilisez l'export syslog, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Consultez la ["Référence aux fichiers journaux"](#) pour plus d'informations sur les journaux StorageGRID. Consultez ["Messages d'audit"](#) pour plus d'informations sur les messages d'audit StorageGRID.

NetApp AutoSupport

La fonctionnalité AutoSupport de StorageGRID vous permet de surveiller de manière proactive l'état de votre système et d'envoyer automatiquement des paquets au site de support NetApp, à l'équipe de support interne de votre organisation ou à un partenaire de support. Par défaut, l'envoi de paquets AutoSupport à NetApp est activé lors de la première configuration de StorageGRID.

La fonctionnalité AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer, car AutoSupport aide à accélérer l'identification et la résolution des problèmes si un incident survient sur votre système StorageGRID.

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison de la nature sensible des paquets AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des paquets AutoSupport à NetApp.

Partage de ressources entre origines (CORS)

Vous pouvez configurer le partage de ressources entre origines (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et les objets qu'il contient soient accessibles aux applications web d'autres

domaines. En règle générale, n'activez pas CORS sauf si cela est requis. Si CORS est requis, limitez-le aux origines de confiance.

Consultez les étapes pour "[Configuration de CORS pour les compartiments et les objets](#)".

Dispositifs de sécurité externes

Une solution de renforcement de sécurité complète doit prendre en compte les mécanismes de sécurité externes à StorageGRID. L'utilisation de dispositifs d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID est un moyen efficace d'établir et de maintenir une posture de sécurité stricte. Ces dispositifs de sécurité externes comprennent les pare-feu, les systèmes de prévention des intrusions (IPS) et d'autres dispositifs de sécurité.

Il est recommandé d'utiliser un répartiteur de charge tiers pour le trafic des clients non fiables. Le répartition de charge tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.

Atténuation des ransomwares

Aidez à protéger vos données objets contre les attaques de ransomware en suivant les recommandations dans "[Défense contre les ransomwares avec StorageGRID](#)".

StorageGRID avec FabricPool

Flux de configuration pour l'utilisation de StorageGRID avec FabricPool

Si vous utilisez le logiciel NetApp ONTAP, vous pouvez utiliser NetApp FabricPool pour transférer les données inactives vers un système de stockage d'objets NetApp StorageGRID.

Utilisez ces instructions pour :

- Découvrez les points à prendre en compte et les bonnes pratiques pour configurer StorageGRID pour une charge de travail FabricPool.
- Découvrez comment configurer un système de stockage d'objets StorageGRID pour une utilisation avec FabricPool.
- Découvrez comment fournir les valeurs requises à ONTAP lors de la connexion de StorageGRID en tant que niveau cloud FabricPool.

Guide de démarrage rapide pour la configuration de StorageGRID pour FabricPool

1

Planifiez votre configuration

- Décidez quelle stratégie de hiérarchisation des volumes FabricPool vous utiliserez pour transférer les données ONTAP inactives vers StorageGRID.
- Planifiez et installez un système StorageGRID pour répondre à vos besoins en capacité et en performance de stockage.
- Familiarisez-vous avec le logiciel système StorageGRID, y compris le "[Gestionnaire de grille](#)" et le "[Gestionnaire de locataires](#)".
- Examinez les meilleures pratiques FabricPool pour "[groupes HA](#)", "[équilibre de charge](#)", "[ILM](#)" et "[plus](#)".

- Consultez ces ressources supplémentaires, qui fournissent des détails sur l'utilisation et la configuration ONTAP et FabricPool :

["TR-4598 : FabricPool Best Practices dans ONTAP"](#)

["Documentation ONTAP pour FabricPool"](#)

2

Effectuer les tâches préalables

Obtenez le ["informations nécessaires pour attacher StorageGRID en tant que niveau cloud"](#), y compris :

- adresses IP
- Noms de domaine
- certificat SSL

Vous pouvez, si vous le souhaitez, configurer ["fédération d'identité"](#) et ["authentification unique"](#).

3

Configurer les paramètres de StorageGRID

Utilisez StorageGRID pour obtenir les valeurs dont ONTAP a besoin pour se connecter à la grille.

L'utilisation de la ["FabricPool assistant de configuration"](#) est recommandée et constitue le moyen le plus rapide de configurer tous les éléments, mais vous pouvez également configurer chaque entité manuellement, si nécessaire.

4

Configurer ONTAP et DNS

Utilisez ONTAP pour ["ajouter un niveau cloud"](#) qui utilise les valeurs StorageGRID. Ensuite, ["configurer les entrées DNS"](#) pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

5

Surveiller et gérer

Une fois votre système opérationnel, effectuez les tâches courantes dans ONTAP et StorageGRID pour gérer et surveiller la hiérarchisation des données FabricPool au fil du temps.

Qu'est-ce que FabricPool?

FabricPool est une solution de stockage hybride ONTAP qui utilise un agrégat flash haute performance comme niveau de performance et un stockage objet comme niveau cloud. L'utilisation d'agrégats compatibles FabricPool vous aide à réduire les coûts de stockage sans compromettre les performances, l'efficacité ou la protection.

FabricPool associe un niveau cloud (un stockage d'objets externe, tel que StorageGRID) à un niveau local (un agrégat de stockage ONTAP) afin de créer un ensemble composite de disques. Les volumes à l'intérieur du FabricPool peuvent alors tirer parti de la hiérarchisation en conservant les données actives (chaudes) sur le stockage haute performance (le niveau local) et en transférant les données inactives (froides) vers le stockage d'objets externe (le niveau cloud).

Aucune modification architecturale n'est requise et vous pouvez continuer à gérer vos données et votre environnement applicatif à partir du système de stockage central ONTAP.

Qu'est-ce que StorageGRID ?

NetApp StorageGRID est une architecture de stockage qui gère les données sous forme d'objets, contrairement à d'autres architectures de stockage telles que le stockage de fichiers ou le stockage bloc. Les objets sont conservés dans un conteneur unique (tel qu'un bucket) et ne sont pas imbriqués comme des fichiers dans un répertoire à l'intérieur d'autres répertoires. Bien que le stockage d'objets offre généralement des performances inférieures à celles du stockage de fichiers ou du stockage bloc, il est nettement plus évolutif. Les buckets StorageGRID peuvent contenir des pétaoctets de données et des milliards d'objets.

Pourquoi utiliser StorageGRID comme niveau cloud FabricPool ?

FabricPool peut transférer les données ONTAP vers un certain nombre de fournisseurs de stockage objet, y compris StorageGRID. Contrairement aux clouds publics qui peuvent fixer un nombre maximal d'opérations d'entrée/sortie par seconde (IOPS) au niveau du bucket ou du conteneur, les performances de StorageGRID évoluent avec le nombre de nœuds dans un système. Utiliser StorageGRID comme niveau cloud FabricPool vous permet de conserver vos données froides dans votre propre cloud privé pour des performances optimales et un contrôle total sur vos données.

De plus, aucune licence FabricPool n'est requise lorsque vous utilisez StorageGRID comme niveau cloud.

Informations nécessaires pour connecter StorageGRID en tant que niveau cloud FabricPool

Avant de pouvoir attacher StorageGRID en tant que niveau cloud pour FabricPool, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir certaines valeurs à utiliser dans ONTAP.

De quelles valeurs avez-vous besoin ?

Le tableau suivant présente les valeurs que vous devez configurer dans StorageGRID et la manière dont ces valeurs sont utilisées par ONTAP et le serveur DNS.

Valeur	Où la valeur est configurée	Là où la valeur est utilisée
Adresses IP virtuelles (VIP)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	ONTAP System Manager > Ajouter un niveau cloud
certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	ONTAP System Manager > Ajouter un niveau cloud
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	Entrée DNS
ID de clé d'accès et clé d'accès secrète	StorageGRID > Locataire et compartiment	ONTAP System Manager > Ajouter un niveau cloud

Valeur	Où la valeur est configurée	Là où la valeur est utilisée
Nom du compartiment/conteneur	StorageGRID > Locataire et compartiment	ONTAP System Manager > Ajouter un niveau cloud

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une ou l'autre des manières suivantes pour obtenir les informations nécessaires :

- Utilisez l'"[FabricPool assistant de configuration](#)". L'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un fichier que vous pouvez utiliser pour configurer ONTAP System Manager. L'assistant vous guide à travers les étapes nécessaires et vous aide à garantir que vos paramètres sont conformes aux bonnes pratiques de StorageGRID et de FabricPool.
- Configurez chaque élément manuellement. Ensuite, saisissez les valeurs dans ONTAP System Manager ou l'interface de ligne de commande ONTAP. Procédez comme suit :
 - a. "[Configurez un groupe à haute disponibilité \(HA\) pour FabricPool](#)".
 - b. "[Créer un point de terminaison d'équilibrage de charge pour FabricPool](#)".
 - c. "[Créer un compte locataire pour FabricPool](#)".
 - d. Connectez-vous au compte locataire, puis "[créez le compartiment et les clés d'accès pour l'utilisateur racine](#)".
 - e. Créez une règle ILM pour les données FabricPool et ajoutez-la à vos stratégies ILM actives. Voir "[Configurer ILM pour les données FabricPool](#)".
 - f. Facultativement, "[créez une politique de classification du trafic pour FabricPool](#)".

Utilisez l'assistant d'installation FabricPool

Découvrez l'assistant de configuration FabricPool de StorageGRID

Vous pouvez utiliser l'assistant de configuration FabricPool pour configurer StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool. Après avoir terminé l'assistant de configuration, vous pouvez saisir les informations requises dans ONTAP System Manager.

Quand utiliser l'assistant de configuration FabricPool

L'assistant de configuration FabricPool vous guide à chaque étape de la configuration de StorageGRID pour une utilisation avec FabricPool et configure automatiquement certaines entités pour vous, telles que les politiques ILM et de classification du trafic. Dans le cadre de la finalisation de l'assistant, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux bonnes pratiques StorageGRID et FabricPool.

Si vous disposez des droits d'accès Root, vous pouvez compléter l'assistant de configuration FabricPool lors de votre première utilisation de StorageGRID Grid Manager, ou vous pouvez accéder à l'assistant et le compléter ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement certains ou tous les éléments requis, puis utiliser l'assistant pour rassembler les valeurs dont ONTAP a besoin dans un seul fichier.



Utilisez l'assistant de configuration FabricPool sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

Avant d'utiliser l'assistant

Confirmez que vous avez effectué ces étapes préalables.

Examiner les bonnes pratiques

- Vous avez une compréhension générale du ["informations nécessaires pour attacher StorageGRID en tant que niveau cloud"](#).
- Vous avez examiné les bonnes pratiques FabricPool pour :
 - ["Groupes à haute disponibilité \(HA\)"](#)
 - ["Équilibrage de charge"](#)
 - ["Règles et politique ILM"](#)

Obtenez des adresses IP et configurez des interfaces VLAN

Si vous configurez un groupe HA, vous savez à quels nœuds ONTAP se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le CIDR du sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel (VLAN) pour segmenter le trafic FabricPool, vous avez déjà configuré l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#).

Configurer la fédération d'identité et l'authentification unique (SSO)

Si vous prévoyez d'utiliser la fédération d'identités ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès racine pour le compte locataire qu'ONTAP utilisera. Voir ["Utilisez la fédération d'identités"](#) et ["Configurer l'authentification unique"](#).

Obtenir et configurer les noms de domaine

- Vous savez quel domaine complet (FQDN) utiliser pour StorageGRID. Les entrées du serveur DNS associeront ce FQDN aux adresses IP virtuelles (VIP) du groupe HA que vous créez à l'aide de l'assistant. Voir ["Configurer le serveur DNS"](#).
- Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, vous avez ["noms de domaine de points de terminaison S3 configurés"](#). ONTAP utilise par défaut des URL de type chemin, mais l'utilisation de requêtes de type hébergement virtuel est recommandée.

Passez en revue les exigences relatives à l'équilibreur de charge et au certificat de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID, vous avez consulté les informations générales ["considérations relatives à l'équilibrage de charge"](#). Vous disposez des certificats à importer ou des valeurs nécessaires à la génération d'un certificat.

Si vous prévoyez d'utiliser un point de terminaison d'équilibreur de charge externe (tiers), vous disposez du domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Confirmez la configuration du pool de stockage ILM

Si vous avez initialement installé StorageGRID 11.6 ou une version antérieure, vous avez configuré le pool de stockage que vous utiliserez. En règle générale, vous devez créer un pool de stockage pour chaque site StorageGRID que vous utiliserez pour stocker des données ONTAP.



Cette condition préalable ne s'applique pas si vous avez initialement installé StorageGRID 11.7 ou 11.8. Lorsque vous installez initialement l'une ou l'autre de ces versions, des pools de stockage sont automatiquement créés pour chaque site.

Relation entre ONTAP et la couche cloud StorageGRID

L'assistant FabricPool vous guide tout au long du processus de création d'un niveau cloud StorageGRID unique comprenant un locataire StorageGRID, un ensemble de clés d'accès et un compartiment StorageGRID. Vous pouvez associer ce niveau cloud StorageGRID à un ou plusieurs niveaux locaux ONTAP.

Attacher un seul niveau cloud à plusieurs niveaux locaux dans un cluster est la bonne pratique générale. Toutefois, selon vos besoins, vous pourriez souhaiter utiliser plusieurs compartiments ou même plusieurs locataires StorageGRID pour les niveaux locaux d'un même cluster. L'utilisation de compartiments et de locataires distincts permet d'isoler les données et l'accès aux données entre les niveaux locaux ONTAP, mais la configuration et la gestion sont alors un peu plus complexes.

NetApp ne recommande pas d'associer un seul niveau cloud à des niveaux locaux dans plusieurs clusters.



Pour connaître les bonnes pratiques d'utilisation de StorageGRID avec NetApp MetroCluster™ et FabricPool Mirror, consultez ["TR-4598 : FabricPool Best Practices dans ONTAP"](#).

Facultatif : utilisez un compartiment différent pour chaque niveau local

Pour utiliser plusieurs compartiments pour les niveaux locaux dans un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque niveau cloud partage le même groupe HA, le même point de terminaison d'équilibrage de charge, le même locataire et les mêmes clés d'accès, mais utilise un conteneur différent (compartiment StorageGRID). Procédez comme suit :

1. Depuis StorageGRID Grid Manager, terminez l'assistant de configuration FabricPool pour le premier niveau cloud.
2. Depuis ONTAP System Manager, ajoutez un niveau cloud et utilisez le fichier que vous avez téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Depuis StorageGRID Tenant Manager, connectez-vous au locataire qui a été créé par l'assistant et créez un deuxième compartiment.
4. Exécutez de nouveau l'assistant FabricPool. Sélectionnez le groupe HA existant, le point de terminaison de l'équilibreur de charge et le locataire. Sélectionnez ensuite le nouveau compartiment que vous avez créé manuellement. Créez une nouvelle règle ILM pour le nouveau compartiment et activez une stratégie ILM pour inclure cette règle.
5. Depuis ONTAP, ajoutez un deuxième niveau cloud, mais indiquez le nouveau nom du compartiment.

Facultatif : utilisez un locataire et un compartiment différents pour chaque niveau local

Pour utiliser plusieurs locataires et différents ensembles de clés d'accès pour les niveaux locaux dans un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque niveau cloud partage le même groupe HA, le même point de terminaison d'équilibrage de charge, mais utilise un locataire, des clés d'accès et un conteneur (StorageGRID bucket) différents. Procédez comme suit :

1. Depuis StorageGRID Grid Manager, terminez l'assistant de configuration FabricPool pour le premier niveau cloud.
2. Depuis ONTAP System Manager, ajoutez un niveau cloud et utilisez le fichier que vous avez téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Recommencez l'assistant FabricPool. Sélectionnez le groupe HA existant et le point de terminaison de l'équilibreur de charge. Créez un nouveau locataire et un nouveau compartiment. Créez une nouvelle règle ILM pour le nouveau compartiment et activez une stratégie ILM pour inclure cette règle.
4. Depuis ONTAP, ajoutez un deuxième niveau cloud, mais fournissez la nouvelle clé d'accès, la clé secrète et le nom du compartiment.

Accédez à l'assistant de configuration StorageGRID FabricPool et terminez-le

Vous pouvez utiliser l'assistant de configuration FabricPool pour configurer StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool.

Avant de commencer

- Vous avez examiné le ["considérations et exigences"](#) pour utiliser l'assistant de configuration FabricPool.



Si vous souhaitez configurer StorageGRID pour l'utiliser avec une autre application cliente S3, rendez-vous sur ["Utilisez l'assistant de configuration S3"](#).

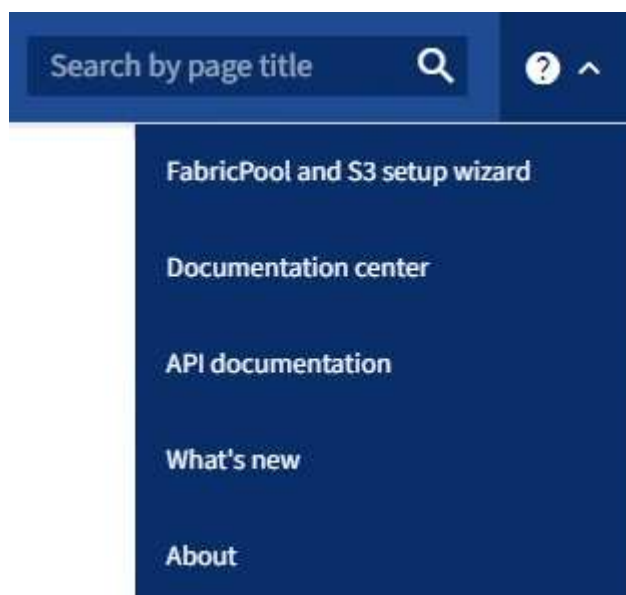
- Vous avez le ["Autorisation d'accès root"](#).

Accédez à l'assistant

Vous pouvez terminer l'assistant de configuration FabricPool lorsque vous commencez à utiliser StorageGRID Grid Manager, ou vous pouvez y accéder et le terminer ultérieurement.

Étapes

1. Connectez-vous au Gestionnaire de grille en utilisant un ["navigateur Web pris en charge"](#).
2. Si la bannière **FabricPool and S3 setup wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du Grid Manager et sélectionnez **FabricPool and S3 setup wizard**.



3. Dans la section FabricPool de la page FabricPool et de l'assistant de configuration S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 9 : Configurer le groupe HA apparaît.

Étape 1 sur 9 : Configurer le groupe HA

Un groupe à haute disponibilité (HA) est un ensemble de nœuds qui contiennent chacun le service d'équilibrage de charge StorageGRID. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe HA pour aider à maintenir les connexions de données FabricPool disponibles. Un groupe HA utilise des adresses IP virtuelles (VIP) pour fournir un accès hautement disponible au service Load Balancer. Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool.

Pour plus de détails sur cette tâche, consultez ["Gérer les groupes à haute disponibilité"](#) et ["Meilleures pratiques pour les groupes à haute disponibilité"](#).

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez à [Étape 2 sur 9 : Configurer le point de terminaison de l'équilibreur de charge](#).
2. Pour utiliser l'équilibreur de charge StorageGRID, créez un nouveau groupe HA ou utilisez un groupe HA existant.

Créer un groupe HA

- Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.
- Pour l'étape **Saisir les détails**, complétez les champs suivants.

Champ	Description
nom de groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

- À l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface par nœud.

- Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toute interface de secours pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs de la colonne **Ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active tombe en panne, les adresses IP virtuelles (VIP) sont transférées vers la première interface de secours dans l'ordre de priorité. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite. Lorsque les pannes sont résolues, les adresses VIP sont réaffectées à l'interface disponible ayant la priorité la plus élevée.

- Pour l'étape **Saisir les adresses IP**, complétez les champs suivants.

Champ	Description
CIDR du sous-réseau	L'adresse du sous-réseau VIP en notation CIDR—une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit comporter aucun bit d'hôte activé. Par exemple, 192.16.0.0/22.
Adresse IP de la passerelle (facultatif)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP de StorageGRID, saisissez l'adresse IP de la passerelle locale VIP de StorageGRID. L'adresse IP de la passerelle locale doit appartenir au sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP et seront toutes actives simultanément sur l'interface active. Au moins une adresse doit être de type IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA** puis **Terminer** pour revenir à l'assistant de configuration FabricPool.

g. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Utiliser le groupe HA existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans la liste déroulante **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Étape 2 sur 9 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes, telles que FabricPool. L'équilibrage de charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID, présent sur tous les nœuds Gateway et Admin, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, consultez la section générale "[considérations relatives à l'équilibrage de charge](#)" et la "[meilleures pratiques pour l'équilibrage de charge pour FabricPool](#)".

Étapes

1. Sélectionnez ou créez un point de terminaison d'équilibrage de charge StorageGRID ou utilisez un équilibreur de charge externe.

Créer un point de terminaison

- a. Sélectionnez **Créer un point de terminaison**.
- b. Pour l'étape **Saisir les détails du point de terminaison**, complétez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous saisissez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Remarque : Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le "Référence du port réseau".
Type de client	Doit être S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : La communication avec StorageGRID sans chiffrement TLS est prise en charge, mais n'est pas recommandée.

- c. À l'étape **Sélectionnez le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le point de terminaison est accessible, soit via n'importe quelle adresse IP, soit via des adresses IP et des interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.

Mode	Description
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.

d. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments. Autoriser tous les locataires est presque toujours l'option appropriée pour le point de terminaison de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous utilisez l'assistant d'installation FabricPool pour un nouveau système StorageGRID et que vous n'avez pas encore créé de comptes locataires.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

e. Pour l'étape **Joindre le certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, la clé privée du certificat et, éventuellement, un ensemble de certificats d'autorité de certification.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les points de terminaison de l'équilibreur de charge" pour plus de détails sur les informations à saisir.
Utiliser le certificat StorageGRID S3	Cette option est disponible uniquement si vous avez déjà importé ou généré une version personnalisée du certificat global StorageGRID. Voir "Configurer les certificats de l'API S3" pour plus de détails.

- f. Sélectionnez **Terminer** pour revenir à l'assistant de configuration FabricPool.
- g. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.



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

Utilisez le point de terminaison de l'équilibreur de charge existant

- a. Sélectionnez le nom d'un point de terminaison existant dans la liste déroulante **Sélectionner un point de terminaison d'équilibrage de charge**.
- b. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Utiliser un équilibreur de charge externe

- a. Complétez les champs suivants pour l'équilibreur de charge externe.

Champ	Description
FQDN	Le domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que FabricPool utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

- b. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Étape 3 sur 9 : Locataire et compartiment

Un locataire est une entité qui peut utiliser des applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités. Vous devez créer un locataire StorageGRID avant de pouvoir créer le compartiment que FabricPool utilisera.

Un bucket est un conteneur utilisé pour stocker les objets et les métadonnées d'un locataire. Bien que certains locataires puissent avoir plusieurs buckets, l'assistant vous permet de créer ou de sélectionner un seul locataire et un seul bucket à la fois. Vous pouvez utiliser le Tenant Manager ultérieurement pour ajouter tous les buckets supplémentaires dont vous avez besoin.

Vous pouvez créer un nouveau locataire et un nouveau compartiment pour l'utilisation de FabricPool, ou vous pouvez sélectionner un locataire et un compartiment existants. Si vous créez un nouveau locataire, le système crée automatiquement l'identifiant de clé d'accès et la clé d'accès secrète pour l'utilisateur racine du locataire.

Pour plus de détails sur cette tâche, consultez ["Créer un compte locataire pour FabricPool"](#) et ["Créez un compartiment S3 et obtenez une clé d'accès"](#).

Étapes

Créez un nouveau locataire et un compartiment ou sélectionnez un locataire existant.

Nouveau locataire et compartiment

1. Pour créer un nouveau locataire et un nouveau compartiment, saisissez un **nom de locataire**. Par exemple, `FabricPool` tenant.
2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise "fédération d'identité", "authentification unique (SSO)" ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir l'autorisation d'accès Root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant auquel vous accordez l'autorisation d'accès Root pour le locataire. Aucun utilisateur local ne peut se connecter.

3. Pour **Nom du compartiment**, saisissez le nom du compartiment que FabricPool utilisera pour stocker les données ONTAP. Par exemple, `fabricpool-bucket`.



Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

4. Sélectionnez la **Région** pour ce compartiment.

Utilisez la région par défaut (`us-east-1`) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer** pour créer le locataire et le compartiment et passer à l'étape de téléchargement des données

Sélectionnez le locataire et le compartiment

Le compte locataire existant doit comporter au moins un compartiment dont le versionnage n'est pas activé. Vous ne pouvez pas sélectionner un compte locataire existant si aucun compartiment n'existe pour ce locataire.

1. Sélectionnez le locataire existant dans la liste déroulante **Nom du locataire**.
2. Sélectionnez le compartiment existant dans la liste déroulante **Nom du compartiment**.

FabricPool ne prend pas en charge le versionnage des objets, de sorte que les compartiments pour lesquels le versionnage est activé ne sont pas affichés.



Ne sélectionnez pas un compartiment pour lequel le verrouillage d'objet S3 est activé pour une utilisation avec FabricPool.

3. Sélectionnez **Continuer** pour passer à l'étape de téléchargement des données.

Étape 4 sur 9 : Télécharger les paramètres ONTAP

Au cours de cette étape, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager.

Étapes

1. Vous pouvez également sélectionner l'icône de copie () pour copier à la fois l'ID de clé d'accès et la clé d'accès secrète dans le presse-papiers.

Ces valeurs sont incluses dans le fichier téléchargé, mais vous pourriez vouloir les enregistrer séparément.

2. Sélectionnez **Download ONTAP settings** pour télécharger un fichier texte contenant les valeurs que vous avez saisies jusqu'à présent.

Le `ONTAP_FabricPool_settings_bucketname.txt` fichier comprend les informations dont vous avez besoin pour configurer StorageGRID en tant que système de stockage d'objets pour un niveau cloud FabricPool, notamment :

- Détails de connexion à l'équilibreur de charge, y compris le nom du serveur (FQDN), le port et le certificat
- Nom du compartiment
- ID de clé d'accès et clé d'accès secrète pour l'utilisateur root du compte locataire

3. Enregistrez les clés copiées et le fichier téléchargé dans un emplacement sécurisé.



Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès, téléchargé les paramètres ONTAP, ou les deux. Les clés ne seront plus disponibles après la fermeture de cette page. Veillez à conserver ces informations en lieu sûr, car elles peuvent être utilisées pour obtenir des données à partir de votre système StorageGRID.

4. Cochez la case pour confirmer que vous avez téléchargé ou copié l'identifiant de la clé d'accès et la clé d'accès secrète.
5. Sélectionnez **Continuer** pour passer à l'étape du pool de stockage ILM.

Étape 5 sur 9 : Sélectionner un pool de stockage

Un pool de stockage est un groupe de nœuds de stockage. Lorsque vous sélectionnez un pool de stockage, vous déterminez les nœuds que StorageGRID utilisera pour stocker les données hiérarchisées depuis ONTAP.

Pour plus de détails sur cette étape, voir "[Créer un pool de stockage](#)".

Étapes

1. Dans la liste déroulante **Site**, sélectionnez le site StorageGRID que vous souhaitez utiliser pour les données hiérarchisées à partir d'ONTAP.
2. Dans la liste déroulante **Pool de stockage**, sélectionnez le pool de stockage pour ce site.

Le pool de stockage d'un site comprend tous les nœuds de stockage de ce site.

3. Sélectionnez **Continuer** pour passer à l'étape de la règle ILM.

Étape 6 sur 9 : Examiner la règle ILM pour FabricPool

Les règles de gestion du cycle de vie de l'information (ILM) contrôlent l'emplacement, la durée et le comportement d'ingestion de tous les objets dans votre système StorageGRID.

L'assistant de configuration FabricPool crée automatiquement la règle ILM recommandée pour l'utilisation de FabricPool. Cette règle s'applique uniquement au compartiment que vous avez spécifié. Elle utilise le code d'effacement 2+1 sur un seul site pour stocker les données hiérarchisées depuis ONTAP.

Pour plus de détails sur cette étape, consultez ["Créer une règle ILM"](#) et ["Meilleures pratiques pour l'utilisation d'ILM avec les données FabricPool"](#).

Étapes

1. Veuillez consulter les détails de la règle.

Champ	Description
Nom de la règle	Généré automatiquement et ne peut pas être modifié
Description	Généré automatiquement et ne peut pas être modifié
Filtre	Le nom du compartiment Cette règle s'applique uniquement aux objets enregistrés dans le compartiment que vous avez spécifié.
Temps de référence	Temps d'ingestion L'instruction de placement commence lorsque les objets sont initialement enregistrés dans le compartiment.
Instructions de placement	Utilisez le code d'effacement 2+1

2. Triez le diagramme de rétention par **Période** et **Pool de stockage** pour confirmer l'instruction de placement.
 - La **Période** pour la règle est **Jour 0 - infini**. **Jour 0** signifie que la règle est appliquée lorsque les données sont transférées par niveau depuis ONTAP. **Infini** signifie que StorageGRID ILM ne supprimera pas les données qui ont été transférées par niveau depuis ONTAP.
 - Le **pool de stockage** associé à la règle est le pool de stockage que vous avez sélectionné. **EC 2+1** signifie que les données seront stockées avec un code d'effacement 2+1. Chaque objet sera enregistré sous la forme de deux fragments de données et d'un fragment de parité. Les trois fragments de chaque objet seront enregistrés sur différents nœuds de stockage d'un même site.
3. Sélectionnez **Créer et continuer** pour créer cette règle et passer à l'étape de la stratégie ILM.

Étape 7 sur 9 : Examiner et activer la politique ILM

Après que l'assistant de configuration FabricPool crée la règle ILM pour l'utilisation de FabricPool, il crée une stratégie ILM. Vous devez soigneusement simuler et examiner cette stratégie avant de l'activer.

Pour plus de détails sur cette étape, voir ["Créer une stratégie ILM"](#) et ["Meilleures pratiques pour l'utilisation d'ILM avec les données FabricPool"](#).



Lorsque vous activez une nouvelle stratégie ILM, StorageGRID utilise cette stratégie pour gérer l'emplacement, la durée et la protection des données de tous les objets dans la grille, y compris les objets existants et les objets nouvellement ingérés. Dans certains cas, l'activation d'une nouvelle stratégie peut entraîner le déplacement d'objets existants vers de nouveaux emplacements.



Pour éviter la perte de données, n'utilisez pas de règle ILM qui expire ou supprime les données du niveau cloud FabricPool. Définissez la période de rétention sur **indéfinie** afin de garantir que les objets FabricPool ne soient pas supprimés par StorageGRID ILM.

Étapes

1. Optionnellement, mettez à jour le **Nom de la politique** généré par le système. Par défaut, le système ajoute "+ FabricPool" au nom de votre politique active ou inactive, mais vous pouvez fournir votre propre nom.
2. Consultez la liste des règles de la politique inactive.
 - Si votre grille ne possède pas de stratégie ILM inactive, l'assistant crée une stratégie inactive en clonant votre stratégie active et en ajoutant la nouvelle règle en haut.
 - Si votre grille possède déjà une stratégie ILM inactive et que cette stratégie utilise les mêmes règles et le même ordre que la stratégie ILM active, l'assistant ajoute la nouvelle règle en haut de la stratégie inactive.
 - Si votre politique inactive contient des règles différentes ou un ordre différent de celui de la politique active, l'assistant crée une nouvelle politique inactive en clonant votre politique active et en ajoutant la nouvelle règle en haut.

3. Examinez l'ordre des règles dans la nouvelle politique inactive.

Parce que la règle FabricPool est la première règle, tous les objets dans le compartiment FabricPool sont placés avant que les autres règles de la politique ne soient évaluées. Les objets dans tout autre compartiment sont placés par les règles suivantes de la politique.

4. Consultez le schéma de rétention pour savoir comment différents objets seront conservés.
 - a. Sélectionnez **Développer tout** pour afficher un diagramme de conservation pour chaque règle de la politique inactive.
 - b. Sélectionnez **Période** et **Pool de stockage** pour consulter le diagramme de rétention. Vérifiez que toutes les règles applicables au compartiment FabricPool ou au locataire conservent les objets **indéfiniment**.
5. Après avoir examiné la politique inactive, sélectionnez **Activer et continuer** pour activer la politique et passer à l'étape de classification du trafic.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irréparable. Examinez attentivement la politique avant de l'activer.

Étape 8 sur 9 : Créez une politique de classification du trafic

En option, l'assistant de configuration FabricPool peut créer une stratégie de classification du trafic que vous pouvez utiliser pour surveiller la charge de travail FabricPool. La stratégie créée par le système utilise une règle de correspondance pour identifier tout le trafic réseau lié au compartiment que vous avez créé. Cette stratégie surveille uniquement le trafic ; elle ne limite pas le trafic pour FabricPool ni pour aucun autre client.

Pour plus de détails sur cette étape, voir ["Créer une politique de classification du trafic pour FabricPool"](#).

Étapes

1. Examinez la politique.
2. Si vous souhaitez créer cette politique de classification du trafic, sélectionnez **Créer et continuer**.

Dès que FabricPool commence à hiérarchiser les données vers StorageGRID, vous pouvez consulter la page Stratégies de classification du trafic pour visualiser les indicateurs de trafic réseau associés à cette stratégie. Par la suite, vous pouvez également ajouter des règles pour limiter d'autres charges de travail et garantir que la charge de travail FabricPool dispose de la majeure partie de la bande passante.

3. Sinon, sélectionnez **Passer cette étape**.

Étape 9 sur 9 : Récapitulatif

Le résumé fournit des détails sur les éléments que vous avez configurés, notamment le nom de l'équilibreur de charge, du locataire et du compartiment, la politique de classification du trafic et la politique ILM active,

Étapes

1. Consultez le résumé.
2. Sélectionnez **Terminer**.

Prochaines étapes

Après avoir terminé l'assistant FabricPool, effectuez ces étapes supplémentaires.

Étapes

1. Accédez à ["Configurer ONTAP System Manager"](#) pour saisir les valeurs enregistrées et compléter la partie ONTAP de la connexion. Vous devez ajouter StorageGRID en tant que niveau cloud, associer le niveau cloud à un niveau local pour créer un FabricPool, et définir les règles de hiérarchisation des volumes.
2. Accédez à ["Configurer le serveur DNS"](#) et assurez-vous que le serveur DNS inclut un enregistrement permettant d'associer le nom du serveur StorageGRID (domaine complet) à chaque adresse IP StorageGRID que vous utiliserez.
3. Accédez à ["Autres bonnes pratiques pour StorageGRID et FabricPool"](#) pour découvrir les bonnes pratiques concernant les journaux d'audit StorageGRID et les autres options de configuration globale.

Configurer StorageGRID manuellement

Créez un groupe à haute disponibilité (HA) pour FabricPool dans StorageGRID

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous pouvez éventuellement créer un ou plusieurs groupes à haute disponibilité (HA). Un groupe HA est un ensemble de nœuds qui contiennent chacun le service d'équilibrage de charge StorageGRID. Un groupe HA peut contenir des nœuds de passerelle, des nœuds

d'administration ou les deux.

Vous pouvez utiliser un groupe HA pour garantir la disponibilité des connexions de données FabricPool. Un groupe HA utilise des adresses IP virtuelles (VIP) pour assurer un accès hautement disponible au service de Load Balancer. Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool.

Pour plus de détails sur cette tâche, consultez "[Gérer les groupes à haute disponibilité](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, rendez-vous sur "[Accédez à l'assistant de configuration FabricPool et terminez-le](#)".

Avant de commencer

- Vous avez examiné le "[bonnes pratiques pour les groupes à haute disponibilité](#)".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".
- Si vous prévoyez d'utiliser un VLAN, vous avez créé l'interface VLAN. Voir "[Configurer les interfaces VLAN](#)".

Étapes

1. Sélectionnez **Configuration > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Create**.
3. Pour l'étape **Saisir les détails**, complétez les champs suivants.

Champ	Description
nom de groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

4. À l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface par nœud.

5. Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toute interface de secours pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs de la colonne **Ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active tombe en panne, les adresses IP virtuelles (VIP) sont transférées vers la première interface de secours dans l'ordre de priorité. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite. Lorsque les pannes sont résolues, les adresses VIP sont réaffectées à l'interface disponible ayant la priorité la plus élevée.

6. Pour l'étape **Saisir les adresses IP**, complétez les champs suivants.

Champ	Description
CIDR du sous-réseau	L'adresse du sous-réseau VIP en notation CIDR—une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit comporter aucun bit d'hôte activé. Par exemple, 192.16.0.0/22.
Adresse IP de la passerelle (facultatif)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP de StorageGRID, saisissez l'adresse IP de la passerelle locale VIP de StorageGRID. L'adresse IP de la passerelle locale doit appartenir au sous-réseau VIP.
Adresse IP virtuelle	Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP. Au moins une adresse doit être de type IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

7. Sélectionnez **Créer un groupe HA** puis sélectionnez **Terminer**.

Créez un point de terminaison d'équilibrage de charge pour FabricPool dans StorageGRID

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes, telles que FabricPool. L'équilibrage de charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous devez configurer un point de terminaison d'équilibrage de charge et télécharger ou générer un certificat de point de terminaison d'équilibrage de charge, qui est utilisé pour sécuriser la connexion entre ONTAP et StorageGRID.

Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à ["Accédez à l'assistant de configuration FabricPool et terminez-le"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).
- Vous avez examiné les aspects généraux ["considérations relatives à l'équilibrage de charge"](#) ainsi que les ["meilleures pratiques pour l'équilibrage de charge pour FabricPool"](#).

Étapes

1. Sélectionnez **Configuration > Réseau > Points de terminaison de l'équilibreur de charge**.
2. Sélectionnez **Create**.
3. Pour l'étape **Saisir les détails du point de terminaison**, complétez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous saisissez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle. Ces ports sont réservés sur les nœuds d'administration. Remarque : Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le "Référence du port réseau". Vous devrez fournir ce numéro à ONTAP lorsque vous connecterez StorageGRID en tant que niveau cloud FabricPool.
Type de client	Sélectionnez S3 .
Protocole réseau	Sélectionnez HTTPS. Remarque : La communication avec StorageGRID sans chiffrement TLS est prise en charge, mais n'est pas recommandée.

4. À l'étape **Sélectionnez le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le point de terminaison est accessible, soit via n'importe quelle adresse IP, soit via des adresses IP et des interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.

Mode	Description
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.

5. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments. Autoriser tous les locataires est presque toujours l'option appropriée pour le point de terminaison de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous n'avez pas encore créé de comptes locataires.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

6. Pour l'étape **Joindre le certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, la clé privée du certificat et, éventuellement, un ensemble de certificats d'autorité de certification.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les points de terminaison de l'équilibreur de charge" pour plus de détails sur les informations à saisir.
Utiliser le certificat StorageGRID S3	Cette option est disponible uniquement si vous avez déjà importé ou généré une version personnalisée du certificat global StorageGRID. Voir "Configurer les certificats de l'API S3" pour plus de détails.

7. Sélectionnez **Create**.



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

Créez un compte locataire pour FabricPool dans StorageGRID

Vous devez créer un compte locataire dans Grid Manager pour l'utilisation de FabricPool.

Les comptes locataires permettent aux applications clientes de stocker et de récupérer des objets sur StorageGRID. Chaque compte locataire possède son propre identifiant de compte, ses groupes et utilisateurs autorisés, ses compartiments et ses objets.

Pour plus de détails sur cette tâche, consultez "[Créer un compte locataire](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, rendez-vous sur "[Accédez à l'assistant de configuration FabricPool et terminez-le](#)".

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez "[autorisations d'accès spécifiques](#)".

Étapes

1. Sélectionnez **Tenants**.
2. Sélectionnez **Create**.
3. Pour les étapes de saisie des détails, saisissez les informations suivantes.

Champ	Description
Nom	Nom du compte locataire. Les noms de locataire n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un identifiant de compte numérique unique.
Description (facultatif)	Une description permettant d'identifier le locataire.
Type de client	Doit être S3 pour FabricPool.
Quota de stockage (facultatif)	Laissez ce champ vide pour FabricPool.

4. Pour l'étape Sélectionner les autorisations :

- a. Ne sélectionnez pas **Autoriser les services de la plateforme**.

FabricPool les locataires n'ont généralement pas besoin d'utiliser les services de la plateforme, tels que la réplication CloudMirror.

- b. Vous pouvez également sélectionner **Utiliser votre propre source d'identité**.

- c. Ne sélectionnez pas **Allow S3 Select**.

FabricPool n'ont généralement pas besoin d'utiliser S3 Select.

- d. Vous pouvez également sélectionner **Utiliser une connexion de fédération de grille** pour permettre au locataire d'utiliser une "[connexion de fédération de grille](#)" pour le clonage de compte et la réplication inter-grilles. Ensuite, sélectionnez la connexion de fédération de grille à utiliser.

5. Pour l'étape Définir l'accès racine, spécifiez quel utilisateur disposera de l'autorisation d'accès racine initiale pour le compte locataire, selon que votre système StorageGRID utilise "[fédération d'identité](#)",

"[authentification unique \(SSO\)](#)" ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir l'autorisation d'accès Root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant auquel vous accordez l'autorisation d'accès Root pour le locataire. Aucun utilisateur local ne peut se connecter.

6. Sélectionnez **Créer un locataire**.

Créez un compartiment S3 et obtenez les clés d'accès pour FabricPool dans StorageGRID

Avant d'utiliser StorageGRID avec une charge de travail FabricPool, vous devez créer un compartiment S3 pour vos données FabricPool. Vous devez également obtenir une clé d'accès et une clé d'accès secrète pour le compte locataire que vous utiliserez pour FabricPool.

Pour plus de détails sur cette tâche, consultez "[Créer un compartiment S3](#)" et "[Créez vos propres clés d'accès S3](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, rendez-vous sur "[Accédez à l'assistant de configuration FabricPool et terminez-le](#)".

Avant de commencer

- Vous avez créé un compte locataire pour l'utilisation de FabricPool.
- Vous disposez d'un accès Root au compte locataire.

Étapes

1. Connectez-vous au Tenant Manager.

Vous pouvez faire l'une ou l'autre des choses suivantes :

- Depuis la page Tenant Accounts dans le Grid Manager, sélectionnez le lien **Sign in** pour le locataire et saisissez vos identifiants.
- Saisissez l'URL du compte locataire dans un navigateur Web et saisissez vos identifiants.

2. Créez un compartiment S3 pour les données FabricPool.

Vous devez créer un compartiment unique pour chaque cluster ONTAP que vous prévoyez d'utiliser.

- Sélectionnez **Afficher les compartiments** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3) > Compartiments**.
- Sélectionnez **Créer un compartiment**.
- Saisissez le nom du compartiment StorageGRID que vous souhaitez utiliser avec FabricPool. Par

exemple, `fabricpool-bucket`.



Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

d. Sélectionnez la région pour ce compartiment.

Par défaut, tous les compartiments sont créés dans la `us-east-1` région. Si la région par défaut est configurée sur une région autre que `us-east-1`, cette autre région est initialement sélectionnée dans la liste déroulante.

e. Sélectionnez **Continuer**.

f. Sélectionnez **Créer un compartiment**.



Ne sélectionnez pas **Activer le versionnage des objets** pour le compartiment FabricPool. De même, ne modifiez pas un compartiment FabricPool pour utiliser **Disponible** ou une cohérence autre que celle par défaut. La cohérence recommandée pour les compartiments FabricPool est **Lecture après nouvelle écriture**, qui est la cohérence par défaut pour un nouveau compartiment.

3. Créez une clé d'accès et une clé d'accès secrète.

a. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.

b. Sélectionnez **Créer une clé**.

c. Sélectionnez **Créer une clé d'accès**.

d. Copiez l'identifiant de la clé d'accès et la clé d'accès secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier tableur contenant l'identifiant de la clé d'accès et la clé d'accès secrète.

Vous saisissez ces valeurs dans ONTAP lorsque vous configurerez StorageGRID en tant que niveau cloud FabricPool.



Si vous générez une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID à l'avenir, saisissez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Sinon, ONTAP pourrait temporairement perdre son accès à StorageGRID.

Configurer StorageGRID ILM pour les données FabricPool

Vous pouvez utiliser cet exemple de politique simple comme point de départ pour vos propres règles et politiques ILM.

Cet exemple suppose que vous concevez les règles ILM et une politique ILM pour un système StorageGRID comportant quatre nœuds de stockage dans un seul centre de données à Denver, Colorado. Les données FabricPool de cet exemple utilisent un compartiment nommé `fabricpool-bucket`.



Les règles et politiques ILM suivantes ne sont données qu'à titre d'exemple. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu afin de protéger le contenu contre la perte. Pour en savoir plus, consultez ["Gérez les objets avec ILM"](#).



Pour éviter la perte de données, n'utilisez pas de règle ILM qui expire ou supprime les données du niveau cloud FabricPool. Définissez la période de rétention sur **indéfinie** afin de garantir que les objets FabricPool ne soient pas supprimés par StorageGRID ILM.

Avant de commencer

- Vous avez examiné le ["bonnes pratiques pour l'utilisation d'ILM avec les données FabricPool"](#).
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès ILM ou Root"](#).
- Si vous avez effectué une mise à niveau vers StorageGRID 12.0 depuis une version de StorageGRID antérieure à 11.7, vous avez configuré le pool de stockage que vous utiliserez. En règle générale, vous devez créer un pool de stockage pour chaque site StorageGRID que vous utiliserez pour stocker des données. (À partir de la version 11.7, les pools de stockage sont créés automatiquement pour chaque site.)



Cette condition préalable ne s'applique pas si vous avez initialement installé StorageGRID 11.7 ou 11.8. Lorsque vous installez initialement l'une ou l'autre de ces versions, des pools de stockage sont automatiquement créés pour chaque site.

Étapes

1. Créez une règle ILM qui s'applique uniquement aux données dans `fabricpool-bucket`. Cette règle d'exemple crée des copies à code d'effacement.

Définition de la règle	Exemple de valeur
Nom de la règle	Code d'effacement 2 + 1 pour les données FabricPool
Nom du compartiment	<code>fabricpool-bucket</code> Vous pouvez également filtrer sur le compte locataire FabricPool.
Filtres avancés	Taille de l'objet supérieure à 0,2 Mo. Remarque : FabricPool n'écrit que des objets de 4 Mo, mais vous devez ajouter un filtre de taille d'objet car cette règle utilise le code d'effacement.
Temps de référence	Temps d'ingestion
Période et emplacements	De Day 0 à toujours Stockez les objets par code d'effacement en utilisant le schéma EC 2+1 à Denver et conservez ces objets dans StorageGRID pour toujours.  Pour éviter la perte de données, n'utilisez pas de règle ILM qui expire ou supprime les données du niveau cloud FabricPool.

Définition de la règle	Exemple de valeur
Comportement d'ingestion	Équilibré

2. Créez une règle ILM par défaut qui créera deux copies répliquées de tout objet non couvert par la première règle. Ne sélectionnez aucun filtre de base (compte locataire ou nom de compartiment) ni aucun filtre avancé.

Définition de la règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Nom du compartiment	<i>none</i>
Filtres avancés	<i>none</i>
Temps de référence	Temps d'ingestion
Période et emplacements	De Day 0 à toujours Stockez les objets en répliquant 2 copies à Denver.
Comportement d'ingestion	Équilibré

3. Créez une stratégie ILM et sélectionnez les deux règles. La règle de réplication n'utilisant aucun filtre, elle peut être la règle par défaut (dernière règle) de la stratégie.
4. Ingérer les objets de test dans la grille.
5. Simulez la règle avec les objets de test pour vérifier le comportement.
6. Activez la règle.

Lorsque cette stratégie est activée, StorageGRID place les données des objets comme suit :

- Les données extraites de FabricPool dans `fabricpool-bucket` seront codées par effacement selon le schéma 2+1. Deux fragments de données et un fragment de parité seront placés sur trois nœuds de stockage différents.
- Tous les objets des autres compartiments seront répliqués. Deux copies seront créées et placées sur deux nœuds de stockage différents.
- Les copies seront conservées dans StorageGRID indéfiniment. StorageGRID ILM ne supprimera pas ces objets.

Créez une politique de classification du trafic pour FabricPool dans StorageGRID

Vous pouvez, si vous le souhaitez, concevoir une politique de classification du trafic StorageGRID afin d'optimiser la qualité de service pour la charge de travail FabricPool.

Pour plus de détails sur cette tâche, consultez ["Gérer les politiques de classification du trafic"](#). Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, rendez-vous sur ["Accédez à l'assistant de configuration FabricPool et terminez-le"](#).

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".

À propos de cette tâche

Les meilleures pratiques pour créer une politique de classification du trafic pour FabricPool dépendent de la charge de travail, comme suit :

- Si vous prévoyez de répartir les données de charge de travail principale FabricPool vers StorageGRID, vous devez vous assurer que la charge de travail FabricPool dispose de la majeure partie de la bande passante. Vous pouvez créer une politique de classification du trafic pour limiter toutes les autres charges de travail.



En général, il est plus important de prioriser les opérations de lecture FabricPool que les opérations d'écriture.

Par exemple, si d'autres clients S3 utilisent ce système StorageGRID, vous devez créer une stratégie de classification du trafic. Vous pouvez limiter le trafic réseau pour les autres compartiments, locataires, sous-réseaux IP ou points de terminaison d'équilibrage de charge.

- En règle générale, vous ne devez pas imposer de limites de qualité de service à une charge de travail FabricPool ; vous ne devez limiter que les autres charges de travail.
- Les limites imposées aux autres charges de travail doivent tenir compte de leur comportement. Les limites imposées varient également en fonction de la taille et des capacités de votre grid, ainsi que du niveau d'utilisation prévu.

Étapes

1. Sélectionnez **Configuration > Réseau > Classification du trafic**.
2. Sélectionnez **Create**.
3. Saisissez un nom et une description (facultatif) pour la règle, puis sélectionnez **Continuer**.
4. À l'étape « Ajouter des règles correspondantes », ajoutez au moins une règle.
 - a. Sélectionnez **Ajouter une règle**
 - b. Pour le type, sélectionnez **Point de terminaison d'équilibrage de charge**, puis sélectionnez le point de terminaison d'équilibrage de charge que vous avez créé pour FabricPool.

Vous pouvez également sélectionner le compte locataire ou le compartiment FabricPool.

- c. Si vous souhaitez que cette politique de trafic limite le trafic pour les autres points de terminaison, sélectionnez **Correspondance inverse**.
5. Vous pouvez, si vous le souhaitez, ajouter une ou plusieurs limites pour contrôler le trafic réseau correspondant à la règle.



StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez comprendre les tendances du trafic.

- a. Sélectionnez **Ajouter une limite**.
 - b. Sélectionnez le type de trafic que vous souhaitez limiter et la limite à appliquer.
6. Sélectionnez **Continue**.

7. Veuillez lire et examiner la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la politique, sélectionnez **Enregistrer et continuer**.

Après avoir terminé

"[Afficher les indicateurs de trafic réseau](#)" pour vérifier que les règles appliquent les limites de trafic que vous attendez.

Configurez ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud FabricPool

Une fois que vous avez obtenu les informations requises StorageGRID, vous pouvez accéder à ONTAP pour ajouter StorageGRID en tant que niveau cloud.

Avant de commencer

- Si vous avez terminé l'assistant de configuration FabricPool, vous avez le fichier `ONTAP_FabricPool_settings_bucketname.txt` que vous avez téléchargé.
- Si vous avez configuré StorageGRID manuellement, vous disposez du nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou de l'adresse IP virtuelle (VIP) du groupe HA StorageGRID, du numéro de port du point de terminaison de l'équilibreur de charge, du certificat de l'équilibreur de charge, de l'ID de clé d'accès et de la clé secrète pour l'utilisateur root du compte locataire, ainsi que du nom du compartiment qu'ONTAP utilisera dans ce locataire.

Accédez à ONTAP System Manager

Ces instructions expliquent comment utiliser ONTAP System Manager pour ajouter StorageGRID comme niveau cloud. Vous pouvez effectuer la même configuration à l'aide de l'interface de ligne de commande ONTAP. Pour obtenir des instructions, allez à "[Documentation ONTAP pour FabricPool](#)".

Étapes

1. Accédez à System Manager pour le cluster ONTAP que vous souhaitez hiérarchiser vers StorageGRID.
2. Connectez-vous en tant qu'administrateur du cluster.
3. Accédez à **STOCKAGE > Niveaux > Ajouter un niveau cloud**.
4. Sélectionnez **StorageGRID** dans la liste des fournisseurs de stockage d'objets.

Saisissez les valeurs StorageGRID

Voir "[Documentation ONTAP pour FabricPool](#)" pour plus d'informations.

Étapes

1. Remplissez le formulaire Ajouter un niveau cloud, en utilisant le `ONTAP_FabricPool_settings_bucketname.txt` fichier ou les valeurs que vous avez obtenues manuellement.

Champ	Description
Nom	Saisissez un nom unique pour ce niveau de cloud. Vous pouvez accepter la valeur par défaut.

Champ	Description
Style d'URL	Si vous "noms de domaine de points de terminaison S3 configurés" sélectionnez URL de type hébergement virtuel. Path-Style URL est le format par défaut pour ONTAP, mais l'utilisation de requêtes de type hébergement virtuel est recommandée pour StorageGRID. Vous devez utiliser Path-Style URL si vous indiquez une adresse IP au lieu d'un nom de domaine pour le champ Server name (FQDN).
Nom du serveur (FQDN)	Saisissez le nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou l'adresse IP virtuelle (VIP) du groupe HA StorageGRID. Par exemple, <code>s3.storagegrid.company.com</code>. Remarque : • L'adresse IP ou le nom de domaine que vous spécifiez ici doit correspondre au certificat que vous avez téléchargé ou généré pour le point de terminaison de l'équilibreur de charge StorageGRID. • Si vous fournissez un nom de domaine, l'enregistrement DNS doit correspondre à chaque adresse IP que vous utiliserez pour vous connecter à StorageGRID. Voir "Configurer le serveur DNS".
SSL	Activé (par défaut).
Certificat de magasin d'objets	Collez le certificat PEM que vous utilisez pour le point de terminaison de l'équilibreur de charge StorageGRID, y compris : <pre>-----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----.</pre> Remarque : Si le certificat StorageGRID a été émis par une autorité de certification intermédiaire, vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.
Port	Saisissez le port utilisé par le point de terminaison de l'équilibreur de charge StorageGRID. ONTAP utilisera ce port lorsqu'il se connectera à StorageGRID. Par exemple, 10433.
Clé d'accès et clé secrète	Saisissez l'ID de clé d'accès et la clé d'accès secrète de l'utilisateur racine du compte locataire StorageGRID. Conseil : Si vous générez ultérieurement une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID, saisissez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Dans le cas contraire, ONTAP risque de perdre temporairement son accès à StorageGRID.
Nom du conteneur	Saisissez le nom du compartiment StorageGRID que vous avez créé pour être utilisé avec ce niveau ONTAP.

2. Finalisez la configuration finale de FabricPool dans ONTAP.
 - a. Associez un ou plusieurs agrégats au niveau cloud.
 - b. Vous pouvez également créer une politique de hiérarchisation des volumes.

Configurer les entrées du serveur DNS pour StorageGRID avec FabricPool

Après avoir configuré les groupes à haute disponibilité, les points de terminaison d'équilibrage de charge et les noms de domaine des points de terminaison S3, vous devez vous assurer que le DNS contient les entrées nécessaires pour StorageGRID. Vous devez inclure une entrée DNS pour chaque nom figurant dans le certificat de sécurité et pour chaque adresse IP que vous pourriez utiliser.

Voir "[Considérations relatives à l'équilibrage de charge](#)".

Entrées DNS pour le nom du serveur StorageGRID

Ajoutez des entrées DNS pour associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez. Les adresses IP que vous saisissez dans le DNS dépendent de l'utilisation ou non d'un groupe HA de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe HA, ONTAP se connectera aux adresses IP virtuelles de ce groupe HA.
- Si vous n'utilisez pas de groupe HA, ONTAP peut se connecter au service d'équilibrage de charge StorageGRID en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration.
- Si le nom du serveur correspond à plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP (jusqu'à un maximum de 16 adresses IP). Les adresses IP sont sélectionnées selon une méthode de type round-robin lors de l'établissement des connexions.

Entrées DNS pour les requêtes de type hébergement virtuel

Si vous avez défini "[Noms de domaine des points de terminaison S3](#)" et que vous utiliserez des requêtes de type hébergement virtuel, ajoutez des entrées DNS pour tous les noms de domaine de point de terminaison S3 requis, y compris tout nom générique.

Meilleures pratiques StorageGRID pour FabricPool

Meilleures pratiques pour les groupes de haute disponibilité (HA) StorageGRID avec FabricPool

Avant d'associer StorageGRID en tant que niveau cloud FabricPool, renseignez-vous sur les groupes de haute disponibilité (HA) de StorageGRID et consultez les bonnes pratiques d'utilisation des groupes HA avec FabricPool.

Qu'est-ce qu'un groupe HA ?

Un groupe haute disponibilité (HA) est un ensemble d'interfaces provenant de plusieurs nœuds StorageGRID Gateway, nœuds d'administration, ou des deux. Un groupe HA permet de maintenir la disponibilité des connexions de données client. Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool.

Chaque groupe HA assure un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe HA composé d'interfaces uniquement sur les nœuds de passerelle ou à la fois sur les

nœuds d'administration et les nœuds de passerelle assure un accès hautement disponible au service d'équilibrage de charge partagé.

Pour en savoir plus sur les groupes à haute disponibilité, consultez ["Gérer les groupes à haute disponibilité \(HA\)"](#).

Utilisation des groupes HA

Les bonnes pratiques pour créer un groupe HA StorageGRID pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec des données de charge de travail principales, vous devez créer un groupe HA comprenant au moins deux nœuds d'équilibrage de charge afin d'éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la stratégie de hiérarchisation des volumes basée uniquement sur les instantanés FabricPool ou des niveaux de performance locaux non principaux (par exemple, des emplacements de reprise après sinistre ou des destinations NetApp SnapMirror®), vous pouvez configurer un groupe HA avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe HA pour Active-Backup HA (un nœud est actif et un nœud est de secours). Cependant, vous pourriez préférer utiliser DNS Round Robin ou Active-Active HA. Pour connaître les avantages de ces autres configurations HA, consultez ["Options de configuration pour les groupes HA"](#).

Meilleures pratiques pour l'équilibrage de charge StorageGRID avec FabricPool

Avant d'associer StorageGRID en tant que niveau cloud FabricPool, consultez les bonnes pratiques d'utilisation des équilibreurs de charge avec FabricPool.

Pour obtenir des informations générales sur l'équilibreur de charge StorageGRID et le certificat de l'équilibreur de charge, consultez ["Considérations relatives à l'équilibrage de charge"](#).

Bonnes pratiques pour l'accès des locataires au point de terminaison de l'équilibreur de charge utilisé pour FabricPool

Vous pouvez contrôler quels locataires peuvent utiliser un point de terminaison d'équilibrage de charge spécifique pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires, en autoriser certains ou en bloquer certains. Lors de la création d'un point de terminaison d'équilibrage de charge pour l'utilisation de FabricPool, sélectionnez **Autoriser tous les locataires**. ONTAP chiffre les données placées dans les compartiments StorageGRID, de sorte que cette couche de sécurité supplémentaire n'apporterait qu'une sécurité additionnelle limitée.

Bonnes pratiques pour le certificat de sécurité

Lorsque vous créez un point de terminaison d'équilibrage de charge StorageGRID pour une utilisation avec FabricPool, vous fournissez le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Dans la plupart des cas, la connexion entre ONTAP et StorageGRID doit utiliser le chiffrement Transport Layer Security (TLS). L'utilisation de FabricPool sans chiffrement TLS est prise en charge, mais n'est pas recommandée. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID, sélectionnez **HTTPS**. Fournissez ensuite le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Pour en savoir plus sur le certificat serveur pour un point de terminaison d'équilibrage de charge :

- ["Gérer les certificats de sécurité"](#)
- ["Considérations relatives à l'équilibrage de charge"](#)
- ["Recommandations pour le renforcement de la sécurité des certificats de serveur"](#)

Ajouter un certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau cloud FabricPool, vous devez installer le même certificat sur le cluster ONTAP, y compris le certificat racine et tous les certificats d'autorité de certification (CA) subordonnés.

Gérer l'expiration des certificats



Si le certificat utilisé pour sécuriser la connexion entre ONTAP et StorageGRID expire, FabricPool cessera temporairement de fonctionner et ONTAP perdra temporairement l'accès aux données hiérarchisées vers StorageGRID.

Pour éviter les problèmes d'expiration de certificat, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que les alertes **Expiration of load balancer endpoint certificate** et **Expiration of global server certificate for S3 API**.
- Veillez à toujours synchroniser les versions StorageGRID et ONTAP du certificat. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le niveau cloud.
- Utilisez un certificat d'autorité de certification (CA) signé publiquement. Si vous utilisez un certificat signé par une CA, vous pouvez utiliser l'API de gestion de la grille pour automatiser la rotation des certificats. Cela vous permet de remplacer les certificats arrivant bientôt à expiration sans interruption de service.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans ONTAP avant l'expiration du certificat existant. Si un certificat auto-signé a déjà expiré, désactivez la validation des certificats dans ONTAP pour éviter toute perte d'accès.

Voir ["NetApp Base de connaissances : Comment configurer un nouveau certificat serveur auto-signé StorageGRID sur un déploiement FabricPool ONTAP existant"](#) pour les instructions.

Meilleures pratiques pour l'utilisation de StorageGRID ILM avec les données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez comprendre les exigences relatives à l'utilisation de la gestion du cycle de vie des informations (ILM) de StorageGRID avec les données FabricPool.



FabricPool n'a aucune connaissance des règles ou politiques ILM de StorageGRID. Une perte de données peut survenir si la politique ILM de StorageGRID est mal configurée. Pour des informations détaillées, consultez ["Utilisez les règles ILM pour gérer les objets"](#) et ["Créer des politiques ILM"](#).

Directives pour l'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant de configuration FabricPool, celui-ci crée automatiquement une nouvelle règle ILM pour chaque compartiment S3 que vous créez et ajoute cette règle à une stratégie inactive. Vous êtes

invité à activer la stratégie. La règle créée automatiquement suit les bonnes pratiques recommandées : elle utilise le code d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant de configuration FabricPool, consultez ces recommandations pour vous assurer que vos règles ILM et votre politique ILM sont adaptées aux données FabricPool et à vos besoins métier. Vous devrez peut-être créer de nouvelles règles et mettre à jour vos politiques ILM actives pour respecter ces recommandations.

- Vous pouvez utiliser n'importe quelle combinaison de règles de réplication et de code d'effacement pour protéger les données du niveau cloud.

La bonne pratique recommandée consiste à utiliser le code d'effacement 2+1 au sein d'un site pour une protection des données rentable. Le code d'effacement utilise davantage de ressources CPU, mais offre une capacité de stockage nettement inférieure à celle de la réplication. Les schémas 4+1 et 6+1 consomment moins de capacité que le schéma 2+1. Cependant, les schémas 4+1 et 6+1 sont moins flexibles si vous devez ajouter des nœuds de stockage lors de l'expansion de la grille. Pour plus de détails, consultez ["Ajouter de la capacité de stockage pour les objets à code d'effacement"](#).

- Chaque règle appliquée aux données FabricPool doit soit utiliser le code d'effacement, soit créer au moins deux copies répliquées.



Une règle ILM qui ne crée qu'une seule copie répliquée pour une période donnée expose les données à un risque de perte définitive. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur significative d'un nœud de stockage. Vous perdez également temporairement l'accès à l'objet lors des procédures de maintenance telles que les mises à niveau.

- Si vous devez ["supprimer les données FabricPool de StorageGRID"](#), utilisez ONTAP pour récupérer toutes les données du volume FabricPool et le promouvoir vers le niveau de performance.



Pour éviter la perte de données, n'utilisez pas de règle ILM qui expire ou supprime les données du niveau cloud FabricPool. Définissez la période de rétention de chaque règle ILM sur **indéfinie** afin de garantir que les objets FabricPool ne soient pas supprimés par StorageGRID ILM.

- Ne créez pas de règles qui déplacent les données du niveau cloud FabricPool hors du compartiment vers un autre emplacement. Vous ne pouvez pas utiliser un Cloud Storage Pool pour déplacer les données FabricPool vers un autre magasin d'objets.



L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence supplémentaire nécessaire pour récupérer un objet depuis la cible du pool de stockage cloud.

- À partir d'ONTAP 9.8, vous pouvez, si vous le souhaitez, créer des étiquettes d'objet pour faciliter la classification et le tri des données hiérarchisées afin d'en simplifier la gestion. Par exemple, vous pouvez définir des étiquettes uniquement sur les volumes FabricPool attachés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous pouvez utiliser le filtre avancé Object Tag pour sélectionner et placer ces données.

Meilleures pratiques pour les paramètres globaux de StorageGRID avec FabricPool

Lors de la configuration d'un système StorageGRID pour une utilisation avec FabricPool, il peut être nécessaire de modifier d'autres options StorageGRID. Avant de modifier un

paramètre global, tenez compte de l'impact de ce changement sur les autres applications S3.

Destinations des messages et journaux d'audit

FabricPool Les charges de travail présentent souvent un taux élevé d'opérations de lecture, ce qui peut générer un volume important de messages d'audit.

- Si vous n'avez pas besoin d'un enregistrement des opérations de lecture client pour FabricPool ou toute autre application S3, vous pouvez accéder à **Configuration > Surveillance > Serveur d'audit et de syslog**. Modifiez le paramètre **Lectures client** sur **Erreur** pour réduire le nombre de messages d'audit enregistrés dans le journal des audits. Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#) pour plus de détails.
- Si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données du journal des audits, configurez un serveur syslog externe et enregistrez les informations d'audit à distance. L'utilisation d'un serveur externe minimise l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir ["Considérations relatives au serveur syslog externe"](#) pour plus de détails.

Chiffrement des objets

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le ["option globale pour le chiffrement des objets stockés"](#) si le chiffrement des données est requis pour d'autres clients StorageGRID. Les données transférées de FabricPool vers StorageGRID sont déjà chiffrées, il n'est donc pas nécessaire d'activer ce paramètre StorageGRID. Les clés de chiffrement côté client sont détenues par ONTAP.

Compression d'objets

Lors de la configuration de StorageGRID, n'activez pas le ["option globale pour compresser les objets stockés"](#). Les données transférées de FabricPool vers StorageGRID sont déjà compressées. L'utilisation de l'option StorageGRID ne réduira pas davantage la taille d'un objet.

Verrouillage d'objet S3

Si le paramètre global S3 Object Lock est activé pour votre système StorageGRID, n'activez pas ["Verrouillage d'objet S3"](#) lors de la création de compartiments FabricPool. S3 Object Lock n'est pas pris en charge pour les compartiments FabricPool.

Cohérence du bucket

Pour les compartiments FabricPool, le niveau de cohérence recommandé est **Read-after-new-write**, qui est le niveau de cohérence par défaut pour un nouveau compartiment. N'éditez pas les compartiments FabricPool pour utiliser **Available** ou **Strong-site**.

Hiérarchisation FabricPool

Si un nœud StorageGRID utilise un stockage attribué à partir d'un système NetApp ONTAP, vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. Par exemple, si un nœud StorageGRID fonctionne sur un hôte VMware, assurez-vous que le volume qui héberge la banque de données pour le nœud StorageGRID n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer des données liées à StorageGRID vers StorageGRID lui-même. Le tiering des données StorageGRID vers StorageGRID augmente la complexité du dépannage et des opérations.

Supprimez les données FabricPool de StorageGRID

Si vous devez supprimer les données FabricPool actuellement stockées dans StorageGRID, vous devez utiliser ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir vers le niveau de performance.

Avant de commencer

- Vous avez pris connaissance des instructions et des considérations dans ["Promouvoir les données vers le niveau de performance"](#).
- Vous utilisez ONTAP 9.8 ou une version ultérieure.
- Vous utilisez un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs StorageGRID pour le compte locataire FabricPool qui possède le ["Gérer tous les compartiments ou autorisation d'accès Root"](#).

À propos de cette tâche

Ces instructions expliquent comment déplacer des données de StorageGRID vers FabricPool. Vous effectuez cette procédure à l'aide de ONTAP et de StorageGRID Tenant Manager.

Étapes

1. Depuis ONTAP, exécutez la commande `volume modify`.

Définissez `tiering-policy` sur `none` pour arrêter la nouvelle hiérarchisation et définissez `cloud-retrieval-policy` sur `promote` pour renvoyer toutes les données précédemment hiérarchisées vers StorageGRID.

Voir ["Promouvoir toutes les données d'un volume FabricPool vers le niveau de performance"](#).

2. Attendez que l'opération soit terminée.

Vous pouvez utiliser la `volume object-store` commande avec l' `tiering` option pour ["vérifiez l'état de la promotion du niveau de performance"](#).

3. Une fois l'opération de promotion terminée, connectez-vous à StorageGRID Tenant Manager pour le compte du locataire FabricPool.
4. Sélectionnez **Afficher les compartiments** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3) > Compartiments**.
5. Confirmez que le seau FabricPool est maintenant vide.
6. Si le seau est vide, ["supprimer le compartiment"](#).

Après avoir terminé

Lorsque vous supprimez le compartiment, la hiérarchisation de FabricPool vers StorageGRID ne peut plus continuer. Cependant, comme le niveau local reste associé au niveau cloud StorageGRID, ONTAP System Manager renverra des messages d'erreur indiquant que le compartiment est inaccessible.

Pour éviter ces messages d'erreur, effectuez l'une des opérations suivantes :

- Utilisez FabricPool Mirror pour connecter un niveau de cloud différent à l'agrégat.
- Déplacez les données de l'agrégat FabricPool vers un agrégat non-FabricPool, puis supprimez l'agrégat inutilisé.

Voir le "[Documentation ONTAP pour FabricPool](#)" pour les instructions.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.