



Meilleures pratiques StorageGRID pour FabricPool

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-120/fabricpool/best-practices-for-high-availability-groups.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Sommaire

- Meilleures pratiques StorageGRID pour FabricPool 1
 - Meilleures pratiques pour les groupes de haute disponibilité (HA) StorageGRID avec FabricPool 1
 - Qu'est-ce qu'un groupe HA ? 1
 - Utilisation des groupes HA 1
 - Meilleures pratiques pour l'équilibrage de charge StorageGRID avec FabricPool 1
 - Bonnes pratiques pour l'accès des locataires au point de terminaison de l'équilibreur de charge utilisé pour FabricPool 2
 - Bonnes pratiques pour le certificat de sécurité 2
 - Meilleures pratiques pour l'utilisation de StorageGRID ILM avec les données FabricPool 3
 - Directives pour l'utilisation d'ILM avec FabricPool 3
 - Meilleures pratiques pour les paramètres globaux de StorageGRID avec FabricPool 4
 - Destinations des messages et journaux d'audit 4
 - Chiffrement des objets 5
 - Compression d'objets 5
 - Verrouillage d'objet S3 5
 - Cohérence du bucket 5
 - Hiérarchisation FabricPool 5

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 équilibrateurs 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'écrivez 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.

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.