Bonnes pratiques StorageGRID pour FabricPool

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-119/fabricpool/best-practices-for-high-availability-groups.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

Bonnes pratiques StorageGRID pour FabricPool

Bonnes pratiques pour les groupes à haute disponibilité (HA)

Avant d'associer StorageGRID en tant que niveau cloud FabricPool , découvrez les groupes haute disponibilité (HA) StorageGRID et examinez les meilleures pratiques d'utilisation des groupes HA avec FabricPool.

Qu'est-ce qu'un groupe HA ?

Un groupe haute disponibilité (HA) est un ensemble d'interfaces provenant de plusieurs nœuds de passerelle StorageGRID , nœuds d'administration ou les deux. Un groupe HA permet de maintenir les connexions de données client disponibles. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool .

Chaque groupe HA fournit un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe HA composé d'interfaces uniquement sur des nœuds de passerelle ou sur des nœuds d'administration et des nœuds de passerelle fournit un accès hautement disponible au service d'équilibrage de charge partagé.

Pour en savoir plus sur les groupes de haute disponibilité, consultez"Gérer les groupes de haute disponibilité (HA)" .

Utilisation des groupes HA

Les meilleures pratiques pour créer un groupe StorageGRID HA pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec des données de charge de travail principales, vous devez créer un groupe HA qui inclut au moins deux nœuds d'équilibrage de charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la stratégie de hiérarchisation des volumes de snapshots FabricPool uniquement ou des niveaux de performances locaux non principaux (par exemple, des emplacements de reprise après sinistre ou des destinations NetApp SnapMirror®), vous pouvez configurer un groupe HA avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe HA pour la HA de sauvegarde active (un nœud est actif et un nœud est de sauvegarde). Cependant, vous préférerez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour connaître les avantages de ces autres configurations HA, consultez"Options de configuration pour les groupes HA" .

Bonnes pratiques d'équilibrage de charge pour FabricPool

Avant d'attacher StorageGRID en tant que niveau cloud FabricPool , passez en revue les meilleures pratiques d'utilisation des équilibreurs de charge avec FabricPool.

Pour obtenir des informations générales sur l'équilibreur de charge StorageGRID et le certificat de l'équilibreur de charge, consultez"Considérations relatives à l'équilibrage de charge" .

Bonnes pratiques pour l'accès des locataires au point de terminaison de l'équilibreur de charge utilisé pour FabricPool

Vous pouvez contrôler quels locataires peuvent utiliser un point de terminaison d'équilibrage de charge spécifique pour accéder à leurs buckets. Vous pouvez autoriser tous les locataires, autoriser certains locataires ou bloquer certains locataires. Lors de la création d'un point de terminaison d'équilibrage de charge pour l'utilisation de FabricPool , sélectionnez **Autoriser tous les locataires**. ONTAP crypte les données placées dans les buckets StorageGRID , donc peu de sécurité supplémentaire serait fournie par cette couche de sécurité supplémentaire.

Bonnes pratiques pour le certificat de sécurité

Lorsque vous créez un point de terminaison d'équilibrage de charge StorageGRID pour l'utilisation de FabricPool , vous fournissez le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Dans la plupart des cas, la connexion entre ONTAP et StorageGRID doit utiliser le cryptage TLS (Transport Layer Security). L'utilisation de FabricPool sans cryptage TLS est prise en charge mais non recommandée. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID , sélectionnez **HTTPS**. Fournissez ensuite le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Pour en savoir plus sur le certificat de serveur pour un point de terminaison d'équilibrage de charge :

- "Gérer les certificats de sécurité"
- "Considérations relatives à l'équilibrage de charge"
- "Directives de renforcement pour les certificats de serveur"

Ajouter un certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau cloud FabricPool , vous devez installer le même certificat sur le cluster ONTAP , y compris les certificats racine et tous les certificats d'autorité de certification (CA) subordonnés.

Gérer l'expiration des certificats

> Si le certificat utilisé pour sécuriser la connexion entre ONTAP et StorageGRID expire, FabricPool cessera temporairement de fonctionner et ONTAP perdra temporairement l'accès aux données hiérarchisées sur StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes qui avertissent de l'approche de la date d'expiration du certificat, telles que les alertes **Expiration du certificat du point de terminaison de l'équilibreur de charge** et **Expiration du certificat du serveur global pour l'API S3**.
- Gardez toujours les versions StorageGRID et ONTAP du certificat synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le niveau cloud.
- Utilisez un certificat CA signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez utiliser l'API de gestion de grille pour automatiser la rotation des certificats. Cela vous permet de remplacer les certificats sur le point d'expirer sans interruption.

- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez remplacer manuellement le certificat dans StorageGRID et dans ONTAP avant l'expiration du certificat existant. Si un certificat auto-signé a déjà expiré, désactivez la validation du certificat dans ONTAP pour éviter toute perte d'accès.

  Voir "Base de connaissances NetApp : Comment configurer un nouveau certificat de serveur auto-signé StorageGRID sur un déploiement ONTAP FabricPool existant" pour les instructions.

Bonnes pratiques pour l'utilisation d'ILM avec les données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez comprendre les exigences d'utilisation de la gestion du cycle de vie des informations (ILM) de StorageGRID avec les données FabricPool .

> FabricPool n'a aucune connaissance des règles ou politiques ILM de StorageGRID . Une perte de données peut se produire si la stratégie ILM StorageGRID est mal configurée. Pour des informations détaillées, voir"Utiliser les règles ILM pour gérer les objets" et"Créer des politiques ILM" .

Directives d'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant de configuration FabricPool , l'assistant crée automatiquement une nouvelle règle ILM pour chaque compartiment S3 que vous créez et ajoute cette règle à une stratégie inactive. Vous êtes invité à activer la politique. La règle créée automatiquement suit les meilleures pratiques recommandées : elle utilise le codage d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant de configuration FabricPool , consultez ces instructions pour vous assurer que vos règles ILM et votre stratégie ILM sont adaptées aux données FabricPool et aux besoins de votre entreprise. Vous devrez peut-être créer de nouvelles règles et mettre à jour vos politiques ILM actives pour respecter ces directives.

- Vous pouvez utiliser n'importe quelle combinaison de règles de réplication et de codage d'effacement pour protéger les données de niveau cloud.

  La meilleure pratique recommandée consiste à utiliser le codage d'effacement 2+1 au sein d'un site pour une protection des données rentable. Le codage d'effacement utilise plus de CPU, mais offre une capacité de stockage nettement inférieure à celle de la réplication. Les schémas 4+1 et 6+1 utilisent moins de capacité que le schéma 2+1. Cependant, les schémas 4+1 et 6+1 sont moins flexibles si vous devez ajouter des nœuds de stockage lors de l'extension du réseau. Pour plus de détails, consultez la section "Ajouter une capacité de stockage pour les objets à code d'effacement" .

- Chaque règle appliquée aux données FabricPool doit soit utiliser le codage d'effacement, soit créer au moins deux copies répliquées.

  > Une règle ILM qui crée une seule copie répliquée pour une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

- Si vous avez besoin de"supprimer les données FabricPool de StorageGRID" , utilisez ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir au niveau de performance.

> Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de niveau cloud FabricPool . Définissez la période de conservation dans chaque règle ILM sur **pour toujours** pour garantir que les objets FabricPool ne sont pas supprimés par StorageGRID ILM.

- Ne créez pas de règles qui déplaceront les données de niveau cloud FabricPool hors du bucket vers un autre emplacement. Vous ne pouvez pas utiliser un pool de stockage cloud pour déplacer les données FabricPool vers un autre magasin d'objets.

> L'utilisation de pools de stockage Cloud avec FabricPool n'est pas prise en charge en raison de la latence supplémentaire nécessaire pour récupérer un objet à partir de la cible du pool de stockage Cloud.

- À partir d' ONTAP 9.8, vous pouvez éventuellement créer des balises d'objet pour aider à classer et trier les données hiérarchisées pour une gestion plus facile. Par exemple, vous pouvez définir des balises uniquement sur les volumes FabricPool attachés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous pouvez utiliser le filtre avancé de balise d'objet pour sélectionner et placer ces données.

Autres bonnes pratiques pour StorageGRID et FabricPool

Lors de la configuration d'un système StorageGRID à utiliser avec FabricPool, vous devrez peut-être modifier d'autres options StorageGRID . Avant de modifier un paramètre global, réfléchissez à la manière dont la modification affectera les autres applications S3.

Destinations des messages d'audit et des journaux

Les charges de travail FabricPool ont souvent un taux élevé d'opérations de lecture, ce qui peut générer un volume élevé de messages d'audit.

- Si vous n'avez pas besoin d'un enregistrement des opérations de lecture client pour FabricPool ou toute autre application S3, accédez éventuellement à **CONFIGURATION** > **Surveillance** > **Serveur d'audit et syslog**. Modifiez le paramètre **Lectures client** sur **Erreur** pour réduire le nombre de messages d'audit enregistrés dans le journal d'audit. Voir"Configurer les messages d'audit et les destinations des journaux" pour plus de détails.
- Si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit, configurez un serveur Syslog externe et enregistrez les informations d'audit à distance. L'utilisation d'un serveur externe minimise l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir"Considérations relatives au serveur syslog externe" pour plus de détails.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le"option globale pour le chiffrement des objets stockés" si le cryptage des données est requis pour d'autres clients StorageGRID . Les données hiérarchisées de FabricPool vers StorageGRID sont déjà chiffrées, l'activation du paramètre StorageGRID n'est donc pas requise. Les clés de chiffrement côté client appartiennent à ONTAP.

Compression d’objets

Lors de la configuration de StorageGRID, n’activez pas le"option globale pour compresser les objets stockés" . Les données hiérarchisées de FabricPool vers StorageGRID sont déjà compressées. L’utilisation de l’option StorageGRID ne réduira pas davantage la taille d’un objet.

Consistance du seau

Pour les buckets FabricPool , la cohérence de bucket recommandée est **Lecture après nouvelle écriture**, qui est la cohérence par défaut pour un nouveau bucket. Ne modifiez pas les buckets FabricPool pour utiliser **Disponible** ou **Strong-site**.

Hiérarchisation de FabricPool

Si un nœud StorageGRID utilise le stockage attribué à partir d’un système NetApp ONTAP , vérifiez que le volume n’a pas de stratégie de hiérarchisation FabricPool activée. Par exemple, si un nœud StorageGRID s’exécute sur un hôte VMware, assurez-vous que le volume qui sauvegarde la banque de données pour le nœud StorageGRID n’a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.

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

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (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.