Meilleures pratiques StorageGRID pour FabricPool

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

Meilleures pratiques StorageGRID pour FabricPool

Bonnes pratiques pour les groupes à haute disponibilité (HA)

Avant de connecter StorageGRID en tant que Tier cloud FabricPool, découvrez les groupes haute disponibilité StorageGRID et consultez les bonnes pratiques d'utilisation des groupes haute disponibilité avec FabricPool.

Qu'est-ce qu'un groupe haute disponibilité ?

Un groupe haute disponibilité est un ensemble d'interfaces issues de plusieurs nœuds de passerelle StorageGRID, nœuds d'administration ou les deux. Un groupe haute disponibilité contribue à maintenir les connexions de données des clients disponibles. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool.

Chaque groupe haute disponibilité fournit un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe haute disponibilité qui se compose d'interfaces uniquement sur les nœuds de passerelle ou sur les deux nœuds d'administration et de passerelle fournit un accès hautement disponible au service Load Balancer partagé.

Pour en savoir plus sur les groupes haute disponibilité, consultez "Gestion des groupes haute disponibilité".

À l'aide de groupes haute disponibilité

Les bonnes pratiques de création de groupe haute disponibilité StorageGRID pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec les données des principaux workloads, vous devez créer un groupe haute disponibilité incluant au moins deux nœuds d'équilibrage de la charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la règle de Tiering de volume FabricPool snapshot uniquement ou des tiers de performance locaux non principaux (par exemple, emplacements de reprise après incident ou destinations NetApp SnapMirror®), vous pouvez configurer un groupe haute disponibilité avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe haute disponibilité pour Active-Backup HA (un nœud est actif et un nœud est une sauvegarde). Cependant, vous préférez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour en savoir plus sur les avantages de ces autres configurations haute disponibilité, reportez-vous "Options de configuration pour les groupes haute disponibilité"à la section .

Bonnes pratiques en matière d'équilibrage de charge pour FabricPool

Avant de rattacher StorageGRID en tant que Tier cloud FabricPool, consultez les bonnes pratiques pour l'utilisation d'équilibreurs de charge avec FabricPool.

Pour plus d'informations générales sur l'équilibreur de charge StorageGRID et le certificat d'équilibreur de

charge, reportez-vous à la section "Considérations relatives à l'équilibrage de charge".

Bonnes pratiques pour l'accès du locataire au terminal d'équilibrage de la charge utilisé pour FabricPool

Vous pouvez contrôler les locataires qui peuvent utiliser un terminal d'équilibrage de la charge spécifique pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires, autoriser certains locataires ou bloquer certains locataires. Lors de la création d'un noeud final d'équilibrage de charge pour l'utilisation de FabricPool, sélectionnez **Autoriser tous les locataires**. ONTAP chiffre les données qui sont placées dans des compartiments StorageGRID. Cette couche de sécurité supplémentaire ne fournit donc que peu de sécurité supplémentaire.

Meilleures pratiques pour le certificat de sécurité

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

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

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

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

Ajouter le certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau de cloud FabricPool, vous devez installer le même certificat sur le cluster ONTAP, y compris le certificat racine et tout certificat d'autorité de certification subordonnée.

Gérer l'expiration des certificats

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

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

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que le **expiration du certificat de noeud final de l'équilibreur de charge** et le **expiration du certificat de serveur global pour les alertes de l'API S3**.
- Gardez toujours les versions StorageGRID et ONTAP du certificat synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le Tier cloud.
- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez utiliser l'API de gestion de grille pour automatiser la rotation des certificats. Vous pouvez ainsi remplacer les certificats dont la date d'expiration arrive à expiration sans

interrompre l'activité.

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

  Voir "Base de connaissances NetApp : comment configurer un nouveau certificat de serveur autosigné StorageGRID sur un déploiement ONTAP FabricPool existant" pour obtenir des instructions.

Bonnes pratiques d'utilisation d'ILM avec des données FabricPool

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

FabricPool ne connaît pas les règles ou les règles ILM de StorageGRID. La perte des données peut se produire si la règle ILM de StorageGRID est mal configurée. Pour plus d'informations, voir "Les règles ILM permettent de gérer les objets" et "Création de règles ILM".

Règles d'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant d'installation FabricPool, il crée automatiquement une règle ILM pour chaque compartiment S3 que vous créez, puis l'ajoute à une règle inactive. Vous êtes invité à activer la stratégie. La règle automatiquement créée respecte les bonnes pratiques recommandées : elle utilise un code d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant d'installation FabricPool, lisez ces instructions pour vous assurer que les règles ILM et la politique ILM sont adaptées aux données FabricPool et aux exigences de votre entreprise. Vous devrez peut-être créer de nouvelles règles et mettre à jour vos règles ILM actives pour répondre à ces instructions.

- Vous pouvez utiliser toutes les combinaisons de réplication et de règles de code d'effacement pour protéger les données de Tier cloud.

  Il est recommandé d'utiliser un code d'effacement 2+1 sur un site pour une protection des données économique. Le code d'effacement consomme plus de ressources de processeur, mais sa capacité de stockage est bien inférieure à la réplication. Les schémas 4+1 et 6+1 utilisent moins de capacité que le schéma 2+1. Toutefois, les schémas 4+1 et 6+1 sont moins flexibles si vous avez besoin d'ajouter des nœuds de stockage lors de l'extension de grid. Pour plus de détails, voir "Ajoutez de la capacité de stockage pour les objets avec code d'effacement".

- Chaque règle appliquée aux données FabricPool doit au moins deux copies répliquées grâce au code d'effacement.

  La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

- Si vous avez besoin de "Supprimez les données FabricPool de StorageGRID", utilisez ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir auprès du Tier de performance.

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

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

> L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.

- Depuis ONTAP 9.8, vous pouvez créer des balises d'objet pour classer et trier les données hiérarchisées pour simplifier la gestion. Par exemple, vous pouvez définir des balises uniquement sur les volumes FabricPool reliés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous pouvez utiliser le filtre avancé balise d'objet pour sélectionner et placer ces données.

Autres meilleures pratiques pour StorageGRID et FabricPool

Lors de la configuration d'un système StorageGRID pour une utilisation avec FabricPool, vous devrez peut-être modifier d'autres options StorageGRID. Avant de modifier un paramètre global, réfléchissez à l'impact de cette modification sur les autres applications S3.

Vérifiez les destinations des messages et des journaux

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

- Si vous n'avez pas besoin d'enregistrer les opérations de lecture du client pour FabricPool ou toute autre application S3, vous pouvez également accéder à **CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**. Définissez le paramètre **lecture client** sur **erreur** pour diminuer le nombre de messages d'audit enregistrés dans le journal d'audit. Voir "Configurez 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 réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir "Considérations relatives au serveur syslog externe" pour plus de détails.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le "option globale de chiffrement des objets stockés" si le chiffrement des données est requis pour d'autres clients StorageGRID. Les données envoyées depuis FabricPool vers StorageGRID sont déjà chiffrées, ce qui signifie qu'il n'est pas nécessaire d'activer le paramètre StorageGRID. Les clés de chiffrement côté client sont la propriété de ONTAP.

Compression d’objet

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

Cohérence du compartiment

Pour les compartiments FabricPool, la cohérence de compartiment recommandée est **Read-After-New-write**, ce qui correspond à la cohérence par défaut d’un nouveau compartiment. Ne modifiez pas les compartiments FabricPool pour utiliser **disponible** ou **site fort**.

Hiérarchisation FabricPool

Si un nœud StorageGRID utilise du stockage attribué à un système NetApp ONTAP, vérifiez qu’aucune règle de hiérarchisation FabricPool n’est activée sur le volume. Par exemple, si un nœud StorageGRID s’exécute sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n’est pas activée sur le volume qui sauvegarde le datastore pour le nœud StorageGRID. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

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

Informations sur le copyright

Informations sur les marques commerciales