Gestion du stockage SAN

ONTAP 9

NetApp
August 14, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/san-admin/san-host-provisioning-concept.html on August 14, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion du stockage SAN . . . 1
Concepts RELATIFS AU SAN . . . 1
Provisionnement DE SAN avec iSCSI . . . 1
Gestion de services iSCSI . . . 2
Provisionnement SAN avec FC . . . 8
Provisionnement SAN avec NVMe . . . 9
Volumes SAN . . . 10
Gestion de l’espace côté hôte SAN . . . 16
À propos des igroups . . . 16
Spécifiez les WWPN des initiateurs et les noms des nœuds iSCSI pour un groupe initiateur . . . 18
Virtualisation du stockage avec copie auxiliaire VMware et Microsoft . . . 18
Administration SAN . . . 25
Provisionnement SAN . . . 25
Provisionnement NVMe . . . 35
Gérer les LUN . . . 48
Gestion des igroups et des ensembles de ports . . . 62
Gérez le protocole iSCSI . . . 68
Gestion du protocole FC . . . 75
Gérez le protocole NVMe . . . 78
Gestion des systèmes avec les adaptateurs FC . . . 89
Gérez les LIF de tous les protocoles SAN . . . 96
Activez l’allocation d’espace ONTAP pour les protocoles SAN . . . 103
Combinaisons de configuration de volumes et de fichiers ou de LUN recommandées . . . 105
Protection des données SAN . . . 111
En savoir plus sur les méthodes de protection des données ONTAP pour les environnements SAN . . . 111
Restaurer une LUN unique à partir d’une copie Snapshot de ONTAP . . . 112
Restaurer toutes les LUN d’un volume à partir d’un snapshot ONTAP . . . 114
Protégez vos données avec des LUN ONTAP FlexClone . . . 115
Configuration et utilisation des sauvegardes SnapVault dans un environnement SAN . . . 116
Configuration recommandée pour connecter un système de sauvegarde hôte à ONTAP . . . 125
Utilisez un système de sauvegarde hôte pour protéger un LUN sur votre système de stockage ONTAP 125
Référence de configuration SAN . . . 127
En savoir plus sur la configuration SAN ONTAP . . . 127
Configurations iSCSI . . . 127
Configurations FC . . . 130
Configurations FCoE . . . 138
Segmentation FC et FCoE . . . 142
Configuration requise pour les hôtes SAN connectés à des systèmes ONTAP et non NetApp . . . 145
Configurations SAN dans un environnement MetroCluster . . . 146
Prise en charge de ONTAP pour les chemins d’accès multiples d’hôtes SAN . . . 149
Limites de configuration . . . 150

Gestion du stockage SAN

Concepts RELATIFS AU SAN

Provisionnement DE SAN avec iSCSI

Dans les environnements SAN, les systèmes de stockage sont des cibles qui disposent de périphériques de stockage cibles. Pour iSCSI et FC, les périphériques cibles de stockage sont appelés LUN (unités logiques). Pour NVMe (non-volatile Memory Express) sur Fibre Channel, les périphériques de stockage cibles sont appelés « namespaces ».

Vous configurez le stockage en créant des LUN pour iSCSI et FC, ou en créant des espaces de noms pour NVMe. Les LUN ou les espaces de noms sont ensuite accessibles par les hôtes via les réseaux de protocole Internet Small Computer Systems interface (iSCSI) ou Fibre Channel (FC).

Pour se connecter aux réseaux iSCSI, les hôtes peuvent utiliser des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte iSCSI dédiés.

Pour la connexion aux réseaux FC, les hôtes nécessitent des HBA FC ou des CNA.

Les protocoles FC pris en charge sont les suivants :

- FC
- FCoE
- NVMe

Noms et connexions réseau du nœud cible iSCSI

Les nœuds cibles iSCSI peuvent se connecter au réseau de plusieurs façons :

- Plus de interfaces Ethernet utilisent un logiciel intégré à ONTAP.
- Via plusieurs interfaces système, avec une interface utilisée pour iSCSI qui transmet également le trafic pour d'autres protocoles, tels que les protocoles SMB et NFS.
- Utilisation d'un adaptateur cible unifié (UTA) ou d'un adaptateur réseau convergé (CNA).

Chaque nœud iSCSI doit avoir un nom de nœud.

Les deux formats, ou les indicateurs de type, pour les noms de nœud iSCSI sont *iqn* et *eui*. La cible iSCSI du SVM utilise toujours l'indicateur de type iqn. L'initiateur peut utiliser l'indicateur de type iqn ou eui.

Nom de nœud du système de stockage

Chaque SVM exécutant iSCSI possède un nom de nœud par défaut basé sur un nom de domaine inverse et un numéro de codage unique.

Le nom du nœud est affiché au format suivant :

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

L'exemple suivant montre le nom de nœud par défaut d'un système de stockage avec un numéro d'encodage

unique :

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Port TCP pour iSCSI

Le protocole iSCSI est configuré dans ONTAP pour utiliser le port TCP numéro 3260.

ONTAP ne prend pas en charge la modification du numéro de port pour iSCSI. Le numéro de port 3260 est enregistré dans le cadre de la spécification iSCSI et ne peut être utilisé par aucune autre application ou service.

Informations associées

"Documentation NetApp : configuration de l'hôte SAN ONTAP"

Gestion de services iSCSI

Gestion de services iSCSI

Vous pouvez gérer la disponibilité du service iSCSI sur les interfaces logiques iSCSI de la machine virtuelle de stockage (SVM) à l'aide de la `vserver iscsi interface enable` ou `vserver iscsi interface disable` commandes.

Par défaut, le service iSCSI est activé sur toutes les interfaces logiques iSCSI.

Mise en œuvre d'iSCSI sur l'hôte

ISCSI peut être implémenté sur l'hôte à l'aide du matériel ou du logiciel.

Vous pouvez implémenter iSCSI de l'une des manières suivantes :

- Utilisation d'un logiciel initiateur qui utilise les interfaces Ethernet standard de l'hôte.
- Via un adaptateur de bus hôte iSCSI (HBA) : un adaptateur HBA iSCSI apparaît au système d'exploitation hôte comme un adaptateur de disque SCSI avec disques locaux.
- Utilisation d'un adaptateur TOE (TCP Offload Engine) qui décharge le traitement TCP/IP.

  Le traitement du protocole iSCSI est toujours exécuté par le logiciel hôte.

Fonctionnement de l'authentification iSCSI

Au cours de la phase initiale d'une session iSCSI, l'initiateur envoie une demande de connexion au système de stockage pour démarrer une session iSCSI. Le système de stockage autorise ou refuse la demande de connexion, ou détermine qu'aucun identifiant n'est requis.

Les méthodes d'authentification iSCSI sont les suivantes :

- CHAP (Challenge Handshake Authentication Protocol) - l'initiateur se connecte à l'aide d'un nom d'utilisateur et d'un mot de passe CHAP.

Vous pouvez spécifier un mot de passe CHAP ou générer un mot de passe hexadécimal secret. Il existe deux types de noms d'utilisateur et de mots de passe CHAP :

- Inbound : le système de stockage authentifie l'initiateur.

  Les paramètres entrants sont requis si vous utilisez l'authentification CHAP.

- Outbound—il s'agit d'un paramètre facultatif permettant à l'initiateur d'authentifier le système de stockage.

  Vous ne pouvez utiliser les paramètres sortants que si vous définissez un nom d'utilisateur et un mot de passe entrants sur le système de stockage.

- Deny—l'accès de l'initiateur est refusé au système de stockage.
- Aucune—le système de stockage ne nécessite pas d'authentification pour l'initiateur.

Vous pouvez définir la liste des initiateurs et leurs méthodes d'authentification. Vous pouvez également définir une méthode d'authentification par défaut qui s'applique aux initiateurs qui ne figurent pas dans cette liste.

Informations associées

"Options Windows de chemins d'accès multiples avec Data ONTAP : Fibre Channel et iSCSI"

Gestion de la sécurité de l'initiateur iSCSI

ONTAP offre un certain nombre de fonctionnalités permettant de gérer la sécurité des initiateurs iSCSI. Vous pouvez définir une liste d'initiateurs iSCSI et la méthode d'authentification pour chacun d'entre eux, afficher les initiateurs et leurs méthodes d'authentification associées dans la liste d'authentification, ajouter et supprimer des initiateurs de la liste d'authentification et définir la méthode d'authentification par défaut de l'initiateur iSCSI pour les initiateurs qui ne figurent pas dans la liste.

Isolation du terminal iSCSI

Les commandes de sécurité iSCSI existantes peuvent accepter une plage d'adresses IP ou plusieurs adresses IP.

Tous les initiateurs iSCSI doivent fournir des adresses IP d'origine lors de l'établissement d'une session ou d'une connexion avec une cible. Cette nouvelle fonctionnalité empêche un initiateur de se connecter au cluster si l'adresse IP d'origine n'est pas prise en charge ou inconnue, fournissant un schéma d'identification unique. Tout initiateur provenant d'une adresse IP non prise en charge ou inconnue aura son login rejeté au niveau de la couche de session iSCSI, empêchant l'initiateur d'accéder à n'importe quelle LUN ou volume du cluster.

Mettez en œuvre cette nouvelle fonctionnalité à l'aide de deux nouvelles commandes pour faciliter la gestion des entrées préexistantes.

Ajouter une plage d'adresses initiateur

Améliorez la gestion de la sécurité de l'initiateur iSCSI en ajoutant une plage d'adresses IP ou plusieurs adresses IP avec le `vserver iscsi security add-initiator-address-range` commande.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Supprimer la plage d'adresses initiateurs

Supprimez une ou plusieurs adresses IP avec le `vserver iscsi security remove-initiator-address-range` commande.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

Qu'est-ce que l'authentification CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) permet une communication authentifiée entre les initiateurs et les cibles iSCSI. Lorsque vous utilisez l'authentification CHAP, vous définissez des noms d'utilisateur et des mots de passe CHAP sur l'initiateur et le système de stockage.

Au cours de la phase initiale d'une session iSCSI, l'initiateur envoie une demande de connexion au système de stockage pour démarrer la session. La demande de connexion inclut le nom d'utilisateur CHAP de l'initiateur et l'algorithme CHAP. Le système de stockage répond par un défi CHAP. L'initiateur fournit une réponse CHAP. Le système de stockage vérifie la réponse et authentifie l'initiateur. Le mot de passe CHAP est utilisé pour calculer la réponse.

Authentification	Appel sortant	Entrant	Correspondre?
Unidirectionnel	Nom d'utilisateur et mot de passe de l'initiateur de l'hôte	Nom d'utilisateur et mot de passe de stockage	Doit correspondre
Bidirectionnel	Nom d'utilisateur et mot de passe de l'initiateur de l'hôte	Nom d'utilisateur et mot de passe de stockage	Doit correspondre
Bidirectionnel	Nom d'utilisateur et mot de passe de stockage	Nom d'utilisateur et mot de passe de l'initiateur de l'hôte	Doit correspondre

Le nom d'utilisateur et le mot de passe sortants de l'initiateur hôte doivent être différents du nom d'utilisateur et du mot de passe sortants du système de stockage.

Consignes d'utilisation de l'authentification CHAP

Vous devez suivre certaines directives lors de l'utilisation de l'authentification CHAP.

- Si vous définissez un nom d'utilisateur et un mot de passe entrants sur le système de stockage, vous devez utiliser le même nom d'utilisateur et le même mot de passe pour les paramètres CHAP sortants sur l'initiateur. Si vous définissez également un nom d'utilisateur et un mot de passe sortants sur le système de stockage pour activer l'authentification bidirectionnelle, vous devez utiliser le même nom d'utilisateur et le même mot de passe pour les paramètres CHAP entrants sur l'initiateur.
- Vous ne pouvez pas utiliser les mêmes nom d'utilisateur et mot de passe pour les paramètres entrant et sortant sur le système de stockage.
- Les noms d'utilisateur CHAP peuvent comporter entre 1 et 128 octets.

  Un nom d'utilisateur nul n'est pas autorisé.

- Les mots de passe CHAP (secrets) peuvent être de 1 à 512 octets.

  Les mots de passe peuvent être des valeurs ou des chaînes hexadécimales. Pour les valeurs

hexadécimales, entrez la valeur avec un préfixe « 0x » ou « 0X ». Un mot de passe nul n'est pas autorisé.

> ONTAP permet d'utiliser des caractères spéciaux, des lettres non anglaises, des chiffres et des espaces pour les mots de passe CHAP (secrets). Toutefois, cette condition est soumise à des restrictions sur les hôtes. Si l'un de ces éléments n'est pas autorisé par votre hôte spécifique, ils ne peuvent pas être utilisés.
>
> Par exemple, l'initiateur logiciel Microsoft iSCSI nécessite que les mots de passe CHAP d'initiateur et de cible soient d'au moins 12 octets si le cryptage IPSec n'est pas utilisé. La longueur maximale du mot de passe est de 16 octets, qu'IPSec soit utilisé ou non.
>
> Si vous souhaitez restrictions supplémentaires, la documentation de l'initiateur doit s'afficher.

Comment utiliser les listes d'accès de l'interface iSCSI pour limiter les interfaces de l'initiateur peut améliorer les performances et la sécurité

Les listes d'accès à l'interface ISCSI peuvent être utilisées pour limiter le nombre de LIF d'un SVM auxquelles un initiateur peut accéder, ce qui améliore les performances et la sécurité.

Lorsqu'un initiateur commence une session de découverte à l'aide d'un iSCSI `SendTargets` Commande, il reçoit les adresses IP associées à la LIF (network interface) qui figurent dans la liste d'accès. Par défaut, tous les initiateurs ont accès à toutes les LIFs iSCSI du SVM. Vous pouvez utiliser la liste d'accès pour limiter le nombre de LIF d'un SVM auquel un initiateur a accès.

ISNS (Internet Storage Name Service) dans ONTAP

Le service iSNS (Internet Storage Name Service) est un protocole qui permet la découverte et la gestion automatisées des périphériques iSCSI sur un réseau de stockage TCP/IP. Un serveur iSNS conserve des informations sur les périphériques iSCSI actifs sur le réseau, y compris leurs adresses IP, les noms d'IQN iSCSI et les groupes de portails.

Vous pouvez obtenir un serveur iSNS auprès d'un fournisseur tiers. Si un serveur iSNS est configuré et activé pour l'initiateur et la cible, vous pouvez utiliser la LIF de gestion d'une machine virtuelle de stockage (SVM) pour enregistrer toutes les LIFs iSCSI de ce SVM sur le serveur iSNS. Une fois l'enregistrement terminé, l'initiateur iSCSI peut interroger le serveur iSNS pour découvrir toutes les LIFs de ce SVM particulier.

Si vous décidez d'utiliser un service iSNS, vous devez vous assurer que vos SVM (Storage Virtual machines) sont correctement enregistrés auprès d'un serveur iSNS (Internet Storage Name Service).

Si vous ne disposez pas d'un serveur iSNS sur votre réseau, vous devez configurer manuellement chaque cible pour qu'elle soit visible par l'hôte.

Que fait un serveur iSNS

Un serveur iSNS utilise le protocole iSNS (Internet Storage Name Service) pour gérer les informations relatives aux périphériques iSCSI actifs sur le réseau, y compris leurs adresses IP, noms de nœuds iSCSI (IQN) et groupes de portails.

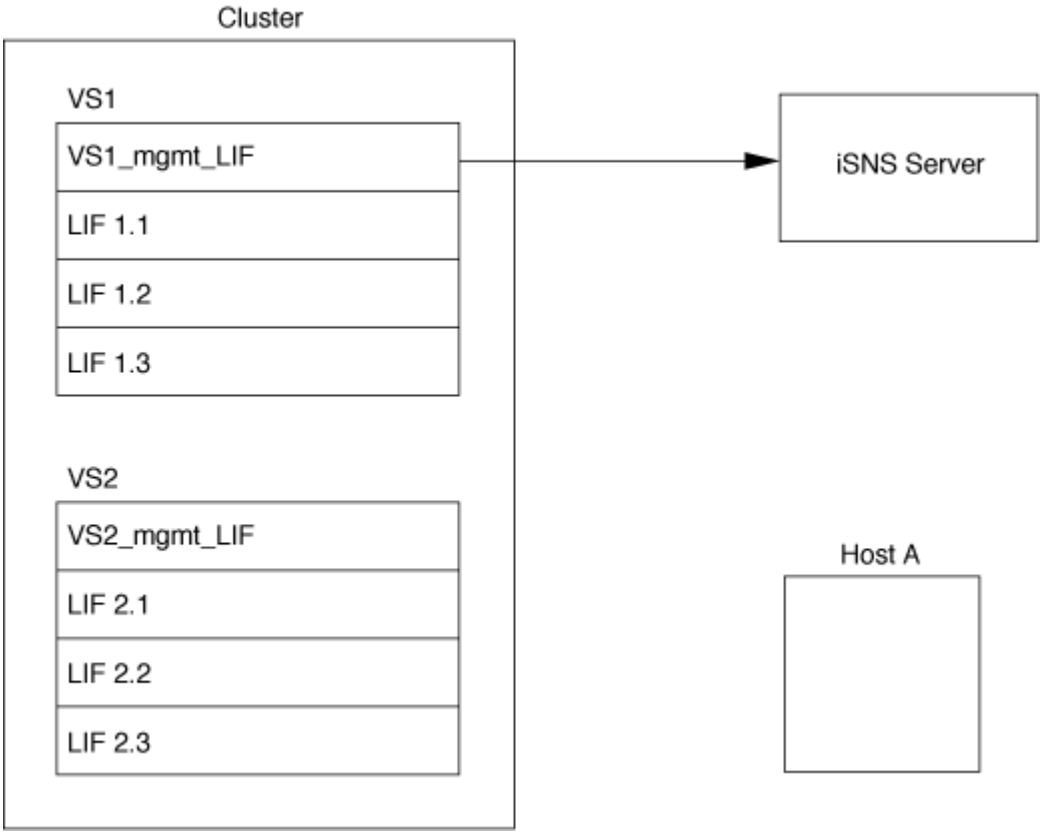
Le protocole iSNS permet la découverte et la gestion automatisées des périphériques iSCSI sur un réseau de stockage IP. Un initiateur iSCSI peut interroger le serveur iSNS pour détecter les périphériques cibles iSCSI.

NetApp ne fournit pas ni ne revende de serveurs iSNS. Vous pouvez obtenir ces serveurs auprès d'un fournisseur pris en charge par NetApp.

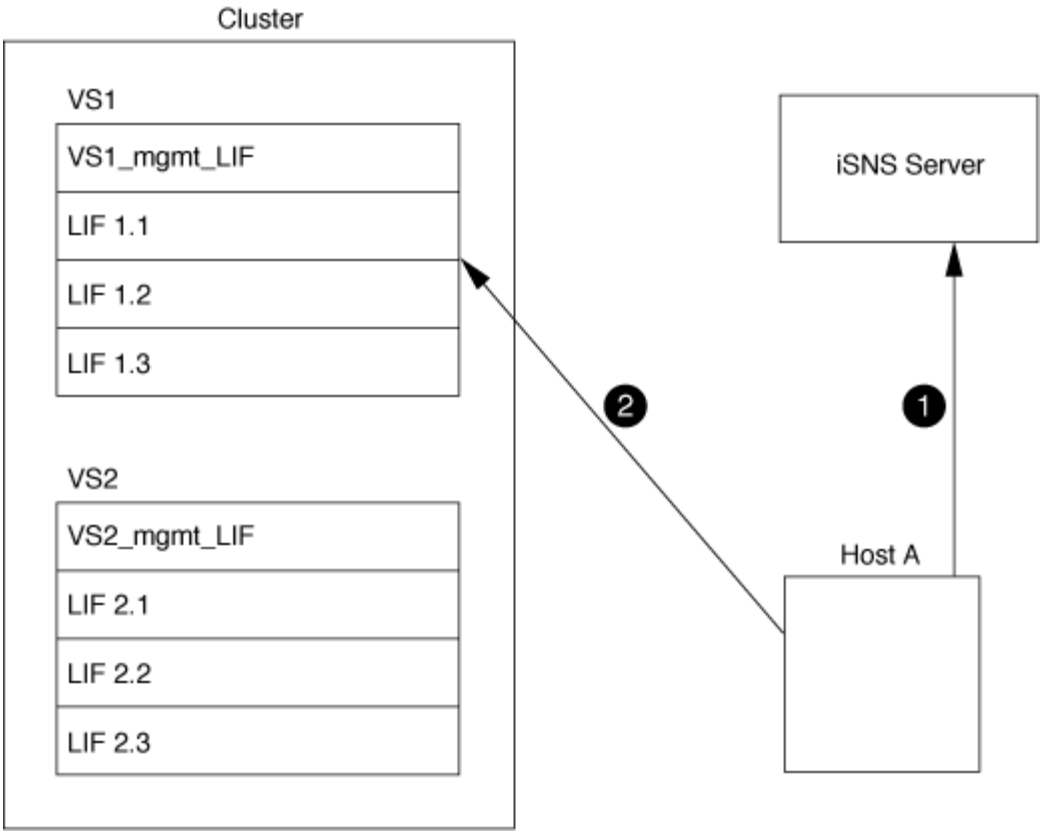
Interaction des SVM avec un serveur iSNS

Le serveur iSNS communique avec chaque machine virtuelle de stockage (SVM) via le LIF de gestion des SVM. La LIF de gestion enregistre toutes les informations de nom de nœud cible iSCSI, d'alias et de portail avec le service iSNS pour un SVM spécifique.

Dans l'exemple suivant, le SVM « VS1 » utilise la LIF de gestion du SVM « VS1_mgmt_lif » pour s'enregistrer sur le serveur iSNS. Lors de l'enregistrement iSNS, un SVM envoie toutes les LIFs iSCSI via le LIF de gestion du SVM au serveur iSNS. Une fois l'enregistrement iSNS terminé, le serveur iSNS dispose d'une liste de toutes les LIFs desservant iSCSI dans « VS1 ». Si un cluster contient plusieurs SVM, chaque SVM doit s'enregistrer individuellement sur le serveur iSNS pour utiliser le service iSNS.



Dans l'exemple suivant, une fois que le serveur iSNS a terminé l'enregistrement avec la cible, l'hôte A peut découvrir toutes les LIFs pour « VS1 » via le serveur iSNS comme indiqué à l'étape 1. Une fois que l'hôte A a terminé la découverte des LIFs pour « VS1 », l'hôte A peut établir une connexion avec l'une des LIFs dans « VS1 », comme indiqué à l'étape 2. L'hôte A ne connaît aucune des LIFs dans « VS2 » jusqu'à ce que la LIF de gestion « VS2_mgmt_LIF » pour les registres « VS2 » avec le serveur iSNS.



Cependant, si vous définissez les listes d'accès de l'interface, l'hôte ne peut utiliser que les LIFs définies dans la liste d'accès de l'interface pour accéder à la cible.

Après la configuration initiale d'iSNS, ONTAP met automatiquement à jour le serveur iSNS lorsque les paramètres de configuration de la SVM changent.

Un délai de quelques minutes peut se produire entre le moment où vous apportez les modifications de configuration et l'envoi de la mise à jour par ONTAP au serveur iSNS. Forcer une mise à jour immédiate des informations iSNS sur le serveur iSNS : `vserver iscsi isns update`. Pour en savoir plus, `vserver iscsi isns update` consultez le "Référence de commande ONTAP".

Commandes de gestion d'iSNS

ONTAP fournit des commandes pour gérer votre service iSNS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurez un service iSNS	`vserver iscsi isns create`
Démarrez un service iSNS	`vserver iscsi isns start`
Modifiez un service iSNS	`vserver iscsi isns modify`
Affiche la configuration du service iSNS	`vserver iscsi isns show`

Forcer une mise à jour des informations iSNS enregistrées	`vserver iscsi isns update`
Arrêtez un service iSNS	`vserver iscsi isns stop`
Supprimez un service iSNS	`vserver iscsi isns delete`
Affichez la page man pour une commande	`man` *`command name`*

Pour en savoir plus, `vserver iscsi isns` consultez le "Référence de commande ONTAP".

Provisionnement SAN avec FC

Vous devez connaître les concepts importants requis pour comprendre comment ONTAP met en œuvre un FC SAN.

Comment les nœuds cibles FC se connectent au réseau

Les systèmes de stockage et les hôtes ont des adaptateurs afin qu'ils puissent être connectés aux commutateurs FC avec des câbles.

Lorsqu'un nœud est connecté au SAN FC, chaque SVM enregistre le WWPN (World Wide Port Name) de sa LIF avec le service Switch Fabric Name. Le WWNN du SVM et le WWPN de chaque LIF sont automatiquement affectés par le ONTAP.

> La connexion directe aux nœuds des hôtes avec FC n'est pas prise en charge, NPIV est requis et un commutateur doit être utilisé.avec les sessions iSCSI, la communication fonctionne avec les connexions soit acheminées par le réseau, soit à connexion directe. Cependant, ces deux méthodes sont prises en charge par ONTAP.

Identification des nœuds FC

Chaque SVM configuré avec FC est identifié par un nom de nœud mondial (WWNN).

Comment les WWPN sont utilisés

Les WWPN identifient chaque LIF dans un SVM configuré pour prendre en charge FC. Ces LIF utilisent les ports FC physiques de chaque nœud du cluster, qui peuvent être des cartes FC target, UTA ou UTA2 configurés comme FC ou FCoE dans les nœuds.

- Création d'un groupe initiateur

  Les WWPN des HBA de l'hôte servent à créer un groupe initiateur. Un groupe initiateur permet de contrôler l'accès des hôtes à des LUN spécifiques. Vous pouvez créer un groupe initiateur en spécifiant une collection de WWPN des initiateurs dans un réseau FC. Lorsque vous mappez une LUN sur un système de stockage sur un groupe initiateur, vous pouvez accorder à tous les initiateurs de ce groupe l'accès à cette LUN. Si le WWPN d'un hôte ne se trouve pas dans un groupe initiateur mappé sur une LUN, cet hôte n'a pas accès à la LUN. Cela signifie que les LUN n'apparaissent pas comme des disques sur cet hôte.

  Vous pouvez également créer des jeux de ports pour rendre une LUN visible uniquement sur des ports

cibles spécifiques. Un ensemble de ports se compose d'un groupe de ports FC target. Vous pouvez lier un groupe initiateur à un ensemble de ports. N'importe quel hôte du groupe initiateur peut accéder aux LUN qu'en vous connectant aux ports cibles de l'ensemble de ports.

- Identification unique des LIF FC

  Les WWPN identifient de manière unique chaque interface logique FC. Le système d'exploitation hôte utilise la combinaison de WWNN et de WWPN pour identifier les SVM et les LIF FC. Certains systèmes d'exploitation nécessitent une liaison permanente pour s'assurer que la LUN apparaît au même ID cible sur l'hôte.

Fonctionnement des affectations de noms à l'échelle mondiale

Les noms dans le monde sont créés de manière séquentielle dans ONTAP. Cependant, en raison de la manière dont ONTAP les affecte, ils peuvent sembler être affectés dans un ordre non séquentiel.

Chaque adaptateur possède un WWPN et un WWNN préconfigurés, mais ONTAP n'utilise pas ces valeurs préconfigurées. En revanche, ONTAP attribue ses propres WWPN ou WWN, en fonction des adresses MAC des ports Ethernet intégrés.

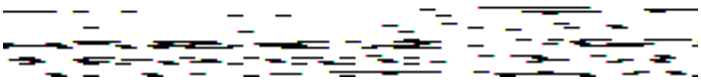
Les noms mondiaux peuvent sembler non séquentiels lorsqu'ils sont affectés pour les raisons suivantes :

- Des noms mondiaux sont attribués à l'ensemble des nœuds et des SVM (Storage Virtual machine) dans le cluster.
- Les noms partout dans le monde libérés sont recyclés et ajoutés au pool de noms disponibles.

Identification des commutateurs FC

Les switchs Fibre Channel possèdent un nom de nœud mondial (WWNN) pour le périphérique lui-même et un WWPN (World Port Name) pour chacun de ses ports.

Le diagramme suivant montre par exemple comment les WWPN sont affectés à chacun des ports d'un commutateur Brocade à 16 ports. Pour plus de détails sur le numéro des ports pour un commutateur particulier, reportez-vous à la documentation fournie par le fournisseur pour ce commutateur.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20: **0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**:00:60:69:51:06:b4

Provisionnement SAN avec NVMe

Depuis la version ONTAP 9.4, NVMe/FC est pris en charge dans un environnement SAN.

NVMe/FC permet aux administrateurs de stockage de provisionner des espaces de noms et des sous-systèmes, puis de les mapper aux sous-systèmes, de la même manière que les LUN sont provisionnées et mappées aux igroups pour FC et iSCSI.

Un namespace NVMe est une quantité de mémoire non volatile pouvant être formatée dans des blocs logiques. Les espaces de noms sont l'équivalent de LUN pour les protocoles FC et iSCSI, et un sous-système NVMe est similaire à un groupe initiateur. Un sous-système NVMe peut être associé à des initiateurs afin que les espaces de noms dans le sous-système soient accessibles par les initiateurs associés.

> Bien qu'ils soient similaires à leur fonction, les espaces de noms NVMe ne prennent pas en charge toutes les fonctionnalités prises en charge par les LUN.

À partir de ONTAP 9.5, une licence est requise pour la prise en charge de l'accès aux données côté hôte avec NVMe. Si NVMe est activé dans ONTAP 9.4, une période de grâce de 90 jours est accordée pour l'acquisition de la licence après la mise à niveau vers ONTAP 9.5. Si vous disposez de "ONTAP One", les licences NVMe sont incluses. Vous pouvez activer la licence à l'aide de la commande suivante :

```
system license add -license-code NVMe_license_key
```

Informations associées

"Rapport technique NetApp 4684 : implémentation et configuration des SAN modernes avec NVMe/FC"

Volumes SAN

Présentation des volumes SAN

ONTAP propose trois options de provisionnement de base : le provisionnement fin, le provisionnement fin et le provisionnement semi-lourd. Chaque option utilise différentes méthodes pour gérer l'espace volume et les besoins en espace pour les technologies de partage de blocs ONTAP. Comprendre le fonctionnement des options vous permet de choisir la meilleure option pour votre environnement.

> Il n'est pas recommandé d'installer des LUN SAN et des partages NAS dans le même volume FlexVol. Vous devez provisionner des volumes FlexVol distincts pour vos LUN SAN, et vous devez en particulier provisionner des volumes FlexVol distincts pour vos partages NAS. Cela simplifie les déploiements de gestion et de réplication, tout en parallèle à la prise en charge des volumes FlexVol dans Active IQ Unified Manager (anciennement OnCommand Unified Manager).

Provisionnement fin pour les volumes

Lors de la création d'un volume à provisionnement fin, ONTAP ne réserve aucun espace supplémentaire lors de la création du volume. Au fur et à mesure de l'écriture des données sur le volume, le volume demande le stockage dont il a besoin depuis l'agrégat pour prendre en charge l'opération d'écriture. L'utilisation de volumes à provisionnement fin vous permet d'effectuer un surengagement de votre agrégat. Ce dernier risque donc de ne pas pouvoir sécuriser l'espace requis lorsqu'il vient à manquer d'espace.

Vous créez un volume FlexVol à provisionnement fin en paramétrant son unité `-space-guarantee` option à `none`.

Provisionnement lourd pour les volumes

Lorsqu'un volume à provisionnement lourd est créé, la mémoire ONTAP réserve suffisamment de stockage de l'agrégat pour garantir l'écriture à tout moment de n'importe quel bloc du volume. Lorsque vous configurez un volume pour utiliser le provisionnement lourd, vous pouvez utiliser n'importe quelle fonction d'efficacité du stockage ONTAP, comme la compression et la déduplication, pour ainsi compenser les plus importantes besoins en stockage initial.

Vous créez un volume FlexVol à provisionnement lourd en définissant sa valeur `-space-slo` (objectif de niveau de service) à `thick`.

Provisionnement semi-lourd pour les volumes

Lorsqu'un volume utilisant un provisionnement semi-lourd est créé, ONTAP met de côté l'espace de stockage de l'agrégat pour tenir compte de la taille du volume. Si l'espace disponible du volume est insuffisant parce que les blocs sont utilisés par les technologies de partage des blocs, ONTAP supprime facilement les objets de données de protection (snapshots, fichiers FlexClone et LUN) afin de libérer l'espace qu'ils conservent. Tant que la ONTAP peut supprimer les objets de données de protection assez rapidement pour prendre en charge l'espace requis pour les écrasements, les opérations d'écriture sont continues. Il s'agit là d'une garantie d'écriture « meilleur effort ».

Remarque : la fonctionnalité suivante n'est pas prise en charge sur les volumes qui utilisent le provisionnement semi-épais :

- Technologies d'efficacité du stockage telles que la déduplication, la compression et la compaction
- Microsoft Offloaded Data Transfer (ODX)

Vous créez un volume FlexVol à provisionnement semi-lourd en paramétrant son option `-space-slo` (objectif de niveau de service) à `semi-thick`.

À utiliser avec des fichiers et des LUN réservés en espace

Une LUN ou un fichier réservé à l'espace est un fichier pour lequel le stockage est alloué lors de sa création. Par le passé, NetApp a utilisé le terme « LUN à provisionnement fin » pour désigner une LUN dont la réservation d'espace est désactivée (LUN non réservée d'espace).

Remarque : les fichiers non réservés à l'espace ne sont généralement pas appelés « fichiers à provisionnement fin ».

Le tableau suivant récapitule les principales différences de manière à utiliser les trois options de provisionnement de volumes avec des fichiers et des LUN réservés à l'espace :

Provisionnement de volume	Réservation d'espace LUN/fichier	Écrasements	Données de protection[2]	Efficacité du stockage[3]
Épais	Pris en charge	Garanti[1]	Résultats garantis	Pris en charge
Fin	Aucun effet	Aucune	Résultats garantis	Pris en charge
Semi-épais	Pris en charge	Meilleur effort[1]	Meilleur effort	Non pris en charge

Notes

1. Pour garantir le remplacement ou fournir une garantie de remplacement sans effort, la réservation d'espace est activée sur la LUN ou le fichier.
2. Les données de protection comprennent les snapshots, ainsi que les fichiers FlexClone et les LUN marqués pour la suppression automatique (clones de sauvegarde).
3. L'efficacité du stockage inclut la déduplication, la compression, tous les fichiers FlexClone et LUN non marqués pour la suppression automatique (clones actifs) et les sous-fichiers FlexClone (utilisés pour le déchargement des copies).

Prise en charge des LUN SCSI à provisionnement fin

ONTAP prend en charge les LUN T10 SCSI à provisionnement fin ainsi que les LUN NetApp à provisionnement fin. Le provisionnement fin SCSI T10 permet aux applications hôtes de prendre en charge les fonctionnalités SCSI, notamment la récupération d'espace LUN et la surveillance de l'espace LUN pour les environnements en blocs. Le provisionnement fin SCSI T10 doit être pris en charge par votre logiciel hôte SCSI.

Vous utilisez ONTAP `space-allocation` Paramètre permettant d'activer/de désactiver la prise en charge du provisionnement fin T10 sur une LUN. Vous utilisez ONTAP `space-allocation enable` Paramètre permettant d'activer le provisionnement fin SCSI T10 sur une LUN.

Le `[-space-allocation {enabled|disabled}]` commande dans le "Référence de commande ONTAP" contient plus d'informations pour activer/désactiver la prise en charge du provisionnement léger T10 et pour activer le provisionnement léger SCSI T10 sur un LUN.

Configurer les options de provisionnement de volumes

Vous pouvez configurer un volume pour le provisionnement fin, le provisionnement lourd ou le provisionnement semi-lourd.

Description de la tâche

Réglage du `-space-slo` option à `thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- 100 % de l'espace requis pour les écrasements est réservé. Vous ne pouvez pas utiliser `volume modify` commande pour configurer les volumes `-fractional-reserve` option

Réglage du `-space-slo` option à `semi-thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- Aucun espace n'est réservé aux écrasements. Vous pouvez utiliser le `volume modify` commande pour configurer les volumes `-fractional-reserve` option.
- La suppression automatique des snapshots est activée.

Étape

1. Configurez les options de provisionnement des volumes :

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

Le `-space-guarantee` par défaut, l'option est `none` Pour les systèmes AFF et pour les volumes non-AFF DP. Sinon, elle est définie par défaut sur `volume`. Pour les volumes FlexVol existants, utilisez le `volume modify` commande permettant de configurer les options de provisionnement.

La commande suivante configure vol1 sur SVM vs1 pour le provisionnement fin :

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
none
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement Thick :

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement semi-lourd :

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

Options de configuration de volume SAN

Vous devez définir différentes options sur le volume contenant votre LUN. La méthode de définition des options du volume détermine la quantité d'espace disponible pour les LUN du volume.

Croissance automatique

Vous pouvez activer ou désactiver la croissance automatique. Si vous la activez, la croissance automatique permet à ONTAP d'augmenter automatiquement la taille du volume jusqu'à une taille maximale que vous prédéterminez. L'espace doit être disponible dans l'agrégat contenant pour prendre en charge la croissance automatique du volume. Par conséquent, si vous activez la croissance automatique, vous devez surveiller l'espace libre dans l'agrégat contenant et en ajouter d'autres si nécessaire.

La croissance automatique ne peut pas être déclenchée pour prendre en charge la création de snapshots. Si vous tentez de créer un snapshot et que l'espace sur le volume est insuffisant, la création du snapshot échoue, même si la croissance automatique est activée.

Si la croissance automatique est désactivée, la taille de votre volume reste la même.

Autoshrink

Vous pouvez activer ou désactiver Autoshrink. Si vous l'activez, la fonction autohrink permet à ONTAP de diminuer automatiquement la taille globale d'un volume lorsque la quantité d'espace consommée dans le volume diminue un seuil prédéfini. Le stockage est ainsi plus efficace, ce qui entraîne le déclenchement des volumes pour libérer automatiquement l'espace libre inutilisé.

Suppression automatique de l'instantané

La suppression automatique des snapshots supprime automatiquement les snapshots lorsque l'une des situations suivantes se produit :

- Le volume est presque plein.
- L'espace de réserve des snapshots est presque plein.
- L'espace de réserve d'écrasement est plein.

Vous pouvez configurer la suppression automatique des instantanés pour supprimer les instantanés de la plus ancienne à la plus récente ou de la plus récente à la plus ancienne. La suppression automatique des snapshots ne supprime pas les snapshots liés aux snapshots dans les volumes ou LUN clonés.

Si votre volume a besoin d'espace supplémentaire et que vous avez activé la suppression automatique de la croissance automatique et de la copie Snapshot, ONTAP tente par défaut d'acquérir l'espace nécessaire en déclenchant d'abord la croissance automatique. Si un espace suffisant n'est pas acquis via la croissance automatique, la suppression automatique de l'instantané est déclenchée.

Réserve Snapshot

La réserve Snapshot définit la quantité d'espace dans le volume réservé pour les snapshots. L'espace alloué à la réserve Snapshot ne peut pas être utilisé à d'autres fins. Si tout l'espace alloué à la réserve de snapshot est utilisé, les snapshots commencent à consommer de l'espace supplémentaire sur le volume.

Nécessité de déplacer des volumes dans des environnements SAN

Avant de déplacer un volume qui contient des LUN ou des espaces de noms, vous devez répondre à certaines exigences.

- Pour les volumes contenant une ou plusieurs LUN, vous devez disposer d'au moins deux chemins par LUN (LIF) qui se connectent à chaque nœud du cluster.

  Cela élimine les points de défaillance uniques et permet au système de résister aux défaillances des composants.

- Pour les volumes contenant des espaces de noms, le cluster doit exécuter ONTAP 9.6 ou version ultérieure.

  Le déplacement de volumes n'est pas pris en charge dans les configurations NVMe qui exécutent ONTAP 9.5.

Considérations relatives à la définition de la réserve fractionnaire

La réserve fractionnaire de remplacement, également appelée *LUN Overwrite Reserve*, permet de désactiver la réserve de remplacements pour les LUN et les fichiers réservés à l'espace dans un volume FlexVol. Cela peut vous aider à optimiser l'utilisation du stockage, mais si votre environnement est affecté par des opérations d'écriture qui échouent à cause du manque d'espace, vous devez comprendre les exigences de cette configuration.

Le paramètre de réserve fractionnaire est exprimé sous forme de pourcentage ; les seules valeurs valides sont `0` et `100` pour cent. Le paramètre de réserve fractionnaire est un attribut du volume.

Définition de la réserve fractionnaire sur `0` meilleure exploitation du stockage. Cependant, une application qui accède aux données d'un volume peut subir une interruption de service des données si son espace est insuffisant, même avec la garantie du volume définie sur `volume`. Toutefois, grâce à une configuration et à une utilisation appropriées du volume, vous pouvez réduire les risques d'échec des écritures. ONTAP propose une garantie d'écriture « meilleur effort » pour les volumes dont la réserve fractionnaire est définie sur `0` lorsque *tous* des conditions suivantes sont remplies :

- La déduplication n'est pas utilisée
- La compression n'est pas utilisée
- Les sous-fichiers FlexClone ne sont pas utilisés
- Tous les fichiers FlexClone et les LUN FlexClone sont activés pour la suppression automatique

  Ce n'est pas le paramètre par défaut. Vous devez explicitement activer la suppression automatique lors de sa création ou en modifiant le fichier FlexClone ou la LUN après sa création.

- ODX et l'allègement de la charge des copies FlexClone ne sont pas utilisés
- La garantie du volume est définie sur `volume`
- La réservation d'espace fichier ou LUN est `enabled`
- La réserve Snapshot du volume est définie sur `0`
- La suppression automatique de l'instantané de volume est `enabled` avec un niveau d'engagement `destroy` de , une liste de destruction `lun_clone,vol_clone,cifs_share,file_clone,sfsr` de et un déclencheur de `volume`

  Ce paramètre permet également de s'assurer que les fichiers FlexClone et les LUN FlexClone sont supprimés lorsque nécessaire.

Notez que si votre taux de modification est élevé, dans de rares cas, la suppression automatique de l'instantané pourrait se trouver en retard, ce qui entraîne un manque d'espace pour le volume, même si tous les paramètres de configuration ci-dessus sont utilisés.

En outre, vous pouvez également utiliser la fonctionnalité de croissance automatique du volume pour réduire le risque de suppression automatique des snapshots de volume. Si vous activez la capacité de croissance automatique, vous devez surveiller l'espace libre dans l'agrégat associé. Si l'agrégat est suffisamment plein pour empêcher la croissance du volume, d'autres snapshots seront probablement supprimés lorsque l'espace libre du volume sera épuisé.

Si vous ne pouvez pas remplir l'ensemble des conditions ci-dessus et que vous devez vous assurer que l'espace du volume est insuffisant, vous devez définir le paramètre de réserve fractionnaire du volume sur `100`. Cela nécessite davantage d'espace disponible à l'avance, mais garantit que les opérations de modification des données réussiront même si les technologies répertoriées ci-dessus sont en cours d'utilisation.

La valeur par défaut et les valeurs autorisées pour le paramètre de réserve fractionnaire dépendent de la garantie du volume :

Garantie de volume	Réserve fractionnaire par défaut	Valeurs autorisées
Volumétrie	100	0, 100

Garantie de volume	Réserve fractionnaire par défaut	Valeurs autorisées
Aucune	0	0, 100

Gestion de l’espace côté hôte SAN

Dans un environnement à provisionnement fin, la gestion de l’espace côté hôte termine le processus de gestion de l’espace du système de stockage libéré dans le système de fichiers hôte.

Un système de fichiers hôte contient des métadonnées pour suivre les blocs disponibles pour stocker de nouvelles données et les blocs contenant des données valides qui ne doivent pas être écrasés. Ces métadonnées sont stockées au sein de la LUN ou du namespace. Lorsqu’un fichier est supprimé dans le système de fichiers hôte, les métadonnées du système de fichiers sont mises à jour pour marquer les blocs de ce fichier comme espace libre. L’espace total disponible du système de fichiers est ensuite recalculé pour inclure les blocs récemment libérés. Sur le système de stockage, ces mises à jour de métadonnées n’apparaissent aucune différence entre les autres écritures effectuées par l’hôte. Par conséquent, le système de stockage n’a pas conscience que des suppressions se sont produits.

Cela crée un écart entre la quantité d’espace libre signalée par l’hôte et la quantité d’espace libre signalée par le système de stockage sous-jacent. Supposons par exemple que vous avez affecté un nouveau LUN de 200 Go provisionné à l’hôte par votre système de stockage. L’hôte et le système de stockage indiquent 200 Go d’espace libre. L’hôte écrit alors 100 Go de données. À ce stade, l’hôte et le système de stockage indiquent 100 Go d’espace utilisé et 100 Go d’espace inutilisé.

Vous supprimez ensuite 50 Go de données de votre hôte. À ce stade, votre hôte indique 50 Go d’espace utilisé et 150 Go d’espace inutilisé. Toutefois, votre système de stockage indique 100 Go d’espace utilisé et 100 Go d’espace inutilisé.

La gestion de l’espace côté hôte utilise différentes méthodes pour concilier la différence d’espace entre l’hôte et le système de stockage.

Gestion simplifiée de l’hôte avec SnapCenter

Le logiciel SnapCenter permet de simplifier certaines des tâches de gestion et de protection des données associées aux solutions de stockage iSCSI et FC. SnapCenter est un package de gestion facultatif pour les hôtes Windows et UNIX.

Le logiciel SnapCenter permet de créer facilement des disques virtuels à partir de pools de stockage qui peuvent être distribués sur plusieurs systèmes de stockage, d’automatiser les tâches de provisionnement du stockage et de simplifier le processus de création de snapshots et de clones à partir de snapshots cohérents avec les données hôte.

Consultez la documentation des produits NetApp pour plus d’informations sur "SnapCenter".

Liens connexes

"Activez l’allocation d’espace ONTAP pour les protocoles SAN"

À propos des igroups

Les groupes initiateurs sont des tableaux des WWPN des hôtes du protocole FC ou des noms des nœuds hôtes iSCSI. Vous pouvez définir des groupes initiateurs et les mapper

sur des LUN pour contrôler l'accès des initiateurs aux LUN.

Généralement, vous souhaitez que tous les ports initiateurs ou initiateurs logiciels de l'hôte puissent accéder à une LUN. Si vous utilisez un logiciel de chemins d'accès multiples ou que vous disposez d'hôtes en cluster, chaque port d'initiateur ou initiateur logiciel de chaque hôte en cluster a besoin de chemins redondants vers la même LUN.

Vous pouvez créer des groupes initiateurs spécifiant les initiateurs auxquels les initiateurs ont accès aux LUN avant ou après leur création. Vous devez toutefois créer des groupes initiateurs avant de pouvoir mapper une LUN sur un groupe initiateur.

Plusieurs groupes initiateurs peuvent avoir plusieurs initiateurs. Vous pouvez également avoir le même initiateur. Toutefois, vous ne pouvez pas mapper une LUN sur plusieurs groupes initiateurs qui ont le même initiateur. Un initiateur ne peut pas être membre des igroups de différents otypes.

Exemple de mode d'accès des groupes initiateurs aux LUN

Vous pouvez créer plusieurs igroups pour définir quels LUN sont disponibles pour vos hôtes. Par exemple, si vous disposez d'un cluster hôte, vous pouvez utiliser des igroups pour s'assurer que des LUN spécifiques ne sont visibles que pour un seul hôte du cluster ou pour tous les hôtes du cluster.

Le tableau suivant montre comment quatre groupes initiateurs accèdent aux LUN pour quatre hôtes différents qui accèdent au système de stockage. Les hôtes en cluster (Host3 et Host4) sont tous deux membres du même groupe initiateur (groupe3) et peuvent accéder aux LUN mappées à ce groupe initiateur. Le groupe initiateur nommé groupe4 contient les WWPN de Host4 pour stocker les informations locales qui ne sont pas destinées à être vues par son partenaire.

Hôtes avec WWPN HBA, IQN ou EUI	igroups	WWPN, IQN et EUI ajoutés aux igroups	LUN mappées aux igroups
Host1, chemin unique (initiateur de logiciel iSCSI) iqn.1991-05.com.microsoft:host1	groupe 1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, multipath (deux HBA) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	groupe 2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3, multipath, cluster avec l'hôte 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	groupe 3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`

Hôtes avec WWPN HBA, IQN ou EUI	igroups	WWPN, IQN et EUI ajoutés aux igroups	LUN mappées aux igroups
Host4, multichemin, cluster (non visible sur Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	groupe4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Spécifiez les WWPN des initiateurs et les noms des nœuds iSCSI pour un groupe initiateur

Lorsque vous créez un groupe initiateur, vous pouvez spécifier les noms des nœuds iSCSI et les WWPN des initiateurs ou les ajouter ultérieurement. Si vous choisissez de spécifier les noms des nœuds iSCSI d'initiateur et les WWPN lorsque vous créez la LUN, ils peuvent être supprimés plus tard, si nécessaire.

Suivez les instructions de la documentation Host Utilities pour obtenir les WWPN et rechercher les noms de nœud iSCSI associés à un hôte spécifique. Pour les hôtes exécutant le logiciel ESX, utilisez Virtual Storage Console.

Virtualisation du stockage avec copie auxiliaire VMware et Microsoft

Présentation de la virtualisation du stockage avec VMware et Microsoft Copy Offload

VMware et Microsoft prennent en charge des opérations de déchargement des copies afin d'augmenter les performances et le débit du réseau. Vous devez configurer votre système pour qu'il réponde aux exigences des environnements des systèmes d'exploitation VMware et Windows et utilise leurs fonctions respectives de déchargement des copies.

Lorsque vous utilisez les copies VMware et Microsoft auxiliaires dans les environnements virtualisés, vos LUN doivent être alignées. Les LUN non alignés peuvent dégrader les performances.

Avantages liés à l'utilisation d'un environnement SAN virtualisé

La création d'un environnement virtualisé à l'aide de serveurs virtuels de stockage (SVM) et de LIF vous permet d'étendre votre environnement SAN à tous les nœuds du cluster.

- Gestion distribuée

  Vous pouvez vous connecter à n'importe quel nœud du SVM afin d'administrer tous les nœuds d'un cluster.

- Un meilleur accès aux données

  Avec MPIO et ALUA, vous avez accès à vos données via n'importe quelle LIF iSCSI ou FC active pour la SVM.

- Contrôle de l’accès aux LUN

  Si vous utilisez SLM et des ensembles de ports, vous pouvez limiter les LIF qu’un initiateur peut utiliser pour accéder aux LUN.

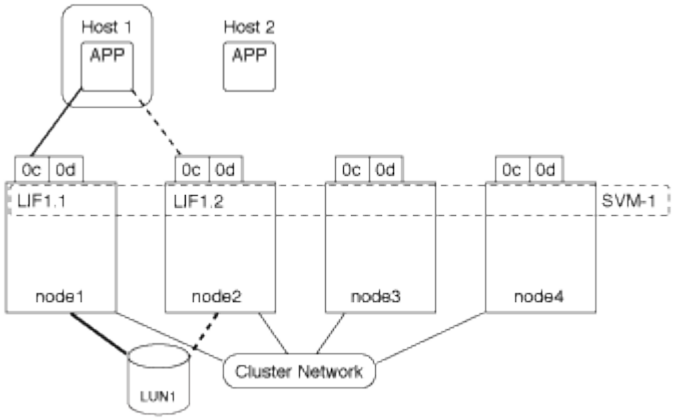
Fonctionnement de l’accès aux LUN dans un environnement virtualisé

Dans un environnement virtualisé, les LIF permettent aux hôtes (clients) d’accéder aux LUN via des chemins optimisés et non optimisés.

Une LIF est une interface logique qui connecte le SVM à un port physique. Bien que plusieurs SVM puissent avoir plusieurs LIF sur le même port, une LIF appartient à un SVM. Vous pouvez accéder aux LUN via les LIFs du SVM.

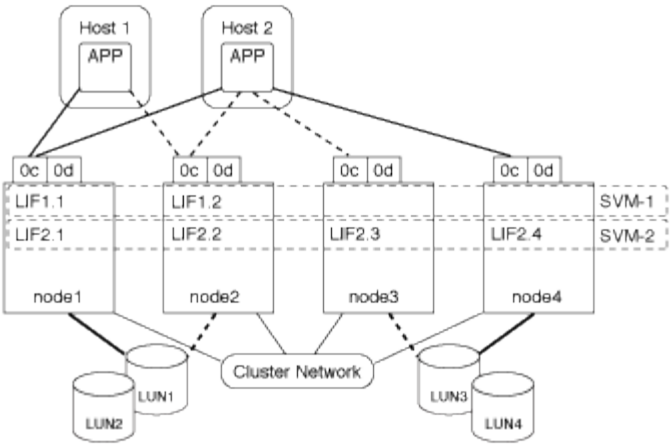
Exemple d’accès à une LUN avec un seul SVM dans un cluster

Dans l’exemple suivant, l’hôte 1 se connecte à LIF1.1 et LIF1.2 au SVM-1 pour accéder à LUN1. LIF1.1 utilise le port physique node1:0C et LIF1.2 utilise le node2:0C. LIF1.1 et LIF1.2 n’appartient qu’au SVM-1. Si une nouvelle LUN est créée sur le nœud 1 ou 2, pour SVM-1, elle peut utiliser ces mêmes LIF. Si un nouveau SVM est créé, de nouvelles LIF peuvent être créées à l’aide des ports physiques 0C ou 0d sur les deux nœuds.



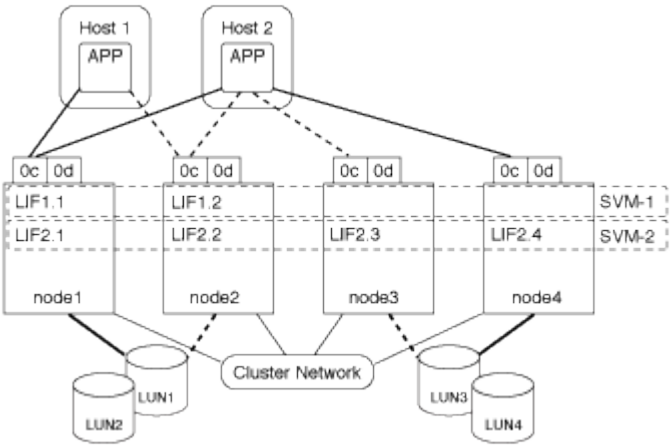
Exemple d’accès LUN avec plusieurs SVM dans un cluster

Un port physique peut prendre en charge plusieurs LIF servant différents SVM. Étant donné que les LIFs sont associées à un SVM particulier, les nœuds de cluster peuvent envoyer le trafic de données entrantes au SVM correct. Dans l’exemple suivant, chaque nœud de 1 à 4 a une LIF pour SVM-2 en utilisant le port physique 0C sur chaque nœud. L’hôte 1 se connecte à LIF1.1 et LIF1.2 du SVM-1 pour accéder à l’utilitaire LUN1. L’hôte 2 se connecte à LIF2-1 et LIF2-2 au SVM-2 pour accéder à LUN2. Les deux SVM partagent le port physique 0C sur les nœuds 1 et 2. SVM-2 dispose de LIF supplémentaires qui utilisent l’hôte 2 pour accéder aux LUN 3 et 4. Ces LIF utilisent le port physique 0C sur les nœuds 3 et 4. Plusieurs SVM peuvent partager les ports physiques sur les nœuds.



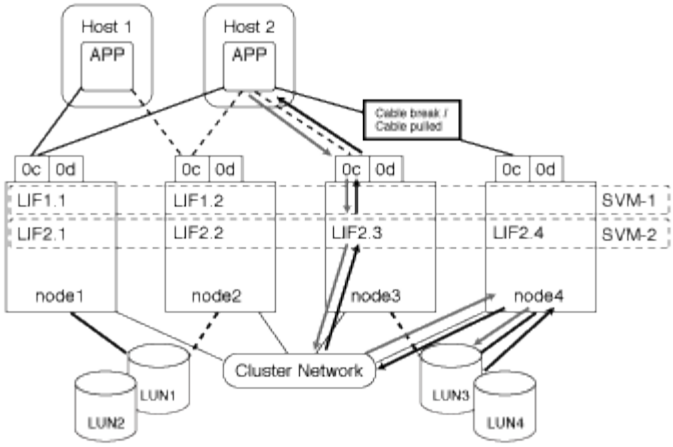
Exemple de chemin actif ou optimisé vers une LUN à partir d'un système hôte

Dans un chemin actif ou optimisé, le trafic de données ne transite pas par le réseau de clusters ; il déplace le chemin le plus direct vers la LUN. Le chemin actif ou optimisé vers LUN1 est via LIF1.1 dans le nœud1, en utilisant le port physique 0C. L'hôte 2 possède deux chemins actifs ou optimisés, un chemin vers le nœud1, LIF2.1, qui partage le port physique 0C et l'autre chemin vers le nœud4, LIF2.4, qui utilise le port physique 0C.



Exemple de chemin d'accès actif ou non optimisé (indirect) vers une LUN depuis un système hôte

Dans un chemin actif ou non optimisé (indirect), le trafic de données transite par le réseau en cluster. Ce problème survient uniquement si tous les chemins actifs ou optimisés d'un hôte ne sont pas disponibles pour gérer le trafic. Si le chemin d'accès de l'hôte 2 vers SVM-2 LIF2.4 est perdu, l'accès à LUN3 et LUN4 traverse le réseau de cluster. L'accès à partir de l'hôte 2 utilise LIF2.3 sur le noeud 3. Ensuite, le trafic entre dans le commutateur de réseau du cluster et sauvegarde vers le nœud4 pour accéder aux LUN3 et LUN4. Il traverse ensuite le commutateur réseau du cluster, puis revient via LIF2.3 à l'hôte 2. Ce chemin actif ou non optimisé est utilisé jusqu'à ce que le chemin vers LIF2.4 soit restauré ou qu'une nouvelle LIF soit créée pour SVM-2 sur un autre port physique du nœud 4.



Améliorer les performances VMware VAAI pour les hôtes ESX

ONTAP prend en charge certaines API VMware vStorage pour l'intégration de baies (VAAI) lorsque l'hôte ESX exécute ESX 4.1 ou une version ultérieure. Ces fonctionnalités permettent de décharger l'hôte ESX vers le système de stockage et d'augmenter le débit du réseau. L'hôte ESX active ces fonctionnalités automatiquement dans l'environnement adéquat.

La fonctionnalité VAAI prend en charge les commandes SCSI suivantes :

- `EXTENDED_COPY`

  Cette fonctionnalité permet à l'hôte de lancer le transfert de données entre les LUN ou au sein d'une LUN sans impliquer l'hôte dans le transfert de données. Résultat : des économies sur les cycles de CPU ESX et une augmentation du débit réseau. La fonctionnalité de copie étendue, également appelée « copie auxiliaire », est utilisée dans les scénarios tels que le clonage d'une machine virtuelle. Lorsqu'elle est invoquée par l'hôte ESX, la fonctionnalité d'allègement de la charge de copie copie copie copie copie copie copie copie copie les données du système de stockage plutôt que de passer par le réseau hôte. L'allègement de la charge des copies transfère les données de l'une des manières suivantes :

  - Dans une LUN
  - Entre les LUN d'un volume
  - Entre des LUN sur des volumes différents au sein d'une machine virtuelle de stockage (SVM)
  - Entre LUN sur différents SVM au sein d'un cluster
    Si cette fonctionnalité ne peut pas être invoquée, l'hôte ESX utilise automatiquement les commandes standard DE LECTURE et D'ÉCRITURE pour l'opération de copie.

- `WRITE_SAME`

  Cette fonctionnalité décharge le travail d'écriture d'un modèle répété, tel que tous les zéros, vers une baie de stockage. L'hôte ESX utilise cette fonctionnalité lors d'opérations telles que le remplissage sans fichier.

- `COMPARE_AND_WRITE`

  Cette fonctionnalité contourne certaines limites de simultanéité d'accès aux fichiers, ce qui accélère les opérations comme le démarrage des machines virtuelles.

Conditions d'utilisation de l'environnement VAAI

Les fonctionnalités VAAI font partie du système d'exploitation ESX et sont automatiquement appelées par l'hôte ESX lors de la configuration de l'environnement approprié.

Les exigences environnementales sont les suivantes :

- L'hôte ESX doit exécuter ESX 4.1 ou version ultérieure.
- Le système de stockage NetApp hébergeant le datastore VMware doit exécuter ONTAP.
- (Copie auxiliaire uniquement) la source et la destination de l'opération de copie VMware doivent être hébergées sur le même système de stockage au sein du même cluster.

> La fonctionnalité d'allègement de la charge des copies ne prend actuellement pas en charge la copie des données entre datastores VMware hébergés sur des systèmes de stockage différents.

Déterminez si les fonctions VAAI sont prises en charge par ESX

Pour vérifier si le système d'exploitation ESX prend en charge les fonctionnalités VAAI, vous pouvez vérifier le client vSphere ou utiliser tout autre moyen d'accéder à l'hôte. ONTAP prend en charge les commandes SCSI par défaut.

Vous pouvez vérifier les paramètres avancés de votre hôte ESX pour déterminer si les fonctionnalités VAAI sont activées. Le tableau indique quelles commandes SCSI correspondent aux noms de contrôle ESX.

Commande SCSI	Nom du contrôle ESX (fonctionnalité VAAI)
COPIE ÉTENDUE	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARER_ET_ÉCRIRE	`HardwareAcceleratedLocking`

Microsoft Offloaded Data Transfer (ODX)

Microsoft Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage ou entre des périphériques de stockage compatibles sans transférer les données via l'ordinateur hôte.

ONTAP prend en charge ODX à la fois pour les protocoles SMB et SAN.

Dans les transferts de fichiers non ODX, les données sont lues à partir de la source et transférées sur le réseau vers l'hôte. L'hôte transfère les données via le réseau vers la destination. Dans le transfert de fichier ODX, les données sont copiées directement de la source vers la destination sans passer par l'hôte.

Les copies déchargées d'ODX sont effectuées directement entre la source et la destination. Par conséquent, des copies sont réalisées au sein d'un même volume pour des performances élevées. Elles offrent notamment une durée de copie plus rapide pour les mêmes copies de volume, une utilisation réduite du processeur et de la mémoire sur le client et une utilisation réduite de la bande passante E/S du réseau. Si les copies se trouvent sur plusieurs volumes, les gains de performances peuvent être négligeables par rapport aux copies basées sur

l'hôte.

Pour les environnements SAN, ODX n'est disponible que lorsqu'il est pris en charge par l'hôte et le système de stockage. Les ordinateurs clients qui prennent en charge ODX et où ODX est activé automatiquement et de manière transparente utilisent le transfert de fichiers déchargées lors du déplacement ou de la copie des fichiers. ODX est utilisé que les fichiers par glisser-déposer soient via l'Explorateur Windows ou qu'il utilise des commandes de copie de fichier en ligne de commande ou qu'une application client lance des demandes de copie de fichiers.

Conditions requises pour l'utilisation d'ODX

Si vous prévoyez d'utiliser ODX pour la réduction des volumes de copies, vous devez connaître les considérations relatives à la prise en charge des volumes, les exigences système et les fonctionnalités logicielles requises.

Pour utiliser ODX, votre système doit disposer des éléments suivants :

- ONTAP

  ODX est automatiquement activé dans les versions prises en charge de ONTAP.

- Volume source minimum de 2 Go

  Pour des performances optimales, le volume source doit être supérieur à 260 Go.

- Prise en charge d'ODX sur le client Windows

  ODX est pris en charge par Windows Server 2012 ou version ultérieure et dans Windows 8 ou version ultérieure. La matrice d'interopérabilité contient les dernières informations sur les clients Windows pris en charge.

  "Matrice d'interopérabilité NetApp"

- Prise en charge des applications de copie pour ODX

  ODX doit être prise en charge par l'application qui effectue le transfert de données. Les opérations applicatives prenant en charge ODX sont les suivantes :

  - Les opérations de gestion Hyper-V, telles que la création et la conversion de disques durs virtuels (VHD), la gestion de snapshots et la copie de fichiers entre des machines virtuelles
  - Opérations de l'Explorateur Windows
  - Commandes de copie Windows PowerShell
  - Commandes de copie de l'invite de commande Windows
    La bibliothèque Microsoft TechNet contient plus d'informations sur les applications ODX prises en charge sur les serveurs et les clients Windows.

- Si vous utilisez des volumes compressés, la taille du groupe de compression doit être de 8 Ko.

  La taille des groupes de compression 32 K n'est pas prise en charge.

ODX ne fonctionne pas avec les types de volume suivants :

- Volumes source d'une capacité inférieure à 2 Go
- Volumes en lecture seule

- "Volumes FlexCache"

  ODX est pris en charge sur les volumes d'origine FlexCache.

- "Volumes provisionnés semi-lourds"

Configuration spéciale pour les fichiers système

Vous pouvez supprimer les fichiers ODX trouvés dans les qtrees. Ne supprimez ou ne modifiez aucun autre fichier système ODX à moins d'en avoir été averti par le support technique.

Lors de l'utilisation de la fonctionnalité ODX, des fichiers système d'ODX existent dans tous les volumes du système. Ces fichiers permettent une représentation instantanée des données utilisées lors du transfert d'ODX. Les fichiers système suivants se trouvent au niveau racine de chaque volume qui contient des LUN ou des fichiers vers lesquels les données ont été déchargées :

- `.copy-offload` (un répertoire masqué)
- `.tokens` (fichier sous le masqué `.copy-offload` répertoire)

Vous pouvez utiliser le `copy-offload delete-tokens -path dir_path -node` *`node_name`* Commande permettant de supprimer un qtree contenant un fichier ODX.

Cas d'utilisation d'ODX

Vous devez tenir compte des cas d'utilisation d'ODX sur des SVM afin de pouvoir déterminer dans quelles circonstances ODX vous fournit des avantages en matière de performances.

Par défaut, les serveurs et clients Windows qui prennent en charge ODX utilisent la fonction d'allègement de la charge des copies pour copier des données sur des serveurs distants. Si le serveur ou le client Windows ne prend pas en charge ODX, ou si l'allègement de la charge des copies ODX échoue à tout moment, l'opération de copie ou de déplacement retourne aux lectures et écritures classiques pour la copie ou le déplacement.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

  Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volume, même nœud, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

  Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

- Inter-cluster

  Les LUN source et de destination se trouvent sur des volumes différents, sur différents nœuds, sur l'ensemble des clusters. Cette fonctionnalité est uniquement prise en charge pour SAN et ne fonctionne pas pour SMB.

Il existe d'autres cas d'utilisation spéciaux :

- Dans l'implémentation de ONTAP ODX, vous pouvez utiliser ODX pour copier des fichiers entre des partages SMB et des disques virtuels connectés FC ou iSCSI.

  Vous pouvez utiliser Windows Explorer, l'interface de ligne de commande Windows ou PowerShell, Hyper-V ou d'autres applications prenant en charge ODX pour copier ou déplacer des fichiers de manière transparente à l'aide de l'allègement de la charge des copies ODX entre les partages SMB et les LUN connectés, à condition que les partages SMB et les LUN soient sur le même cluster.

- Hyper-V fournit des cas d'utilisation supplémentaires pour la décharge de copies ODX :

  - Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

    Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

  - Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
  - L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.

> Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Administration SAN

Provisionnement SAN

Présentation de la gestion SAN

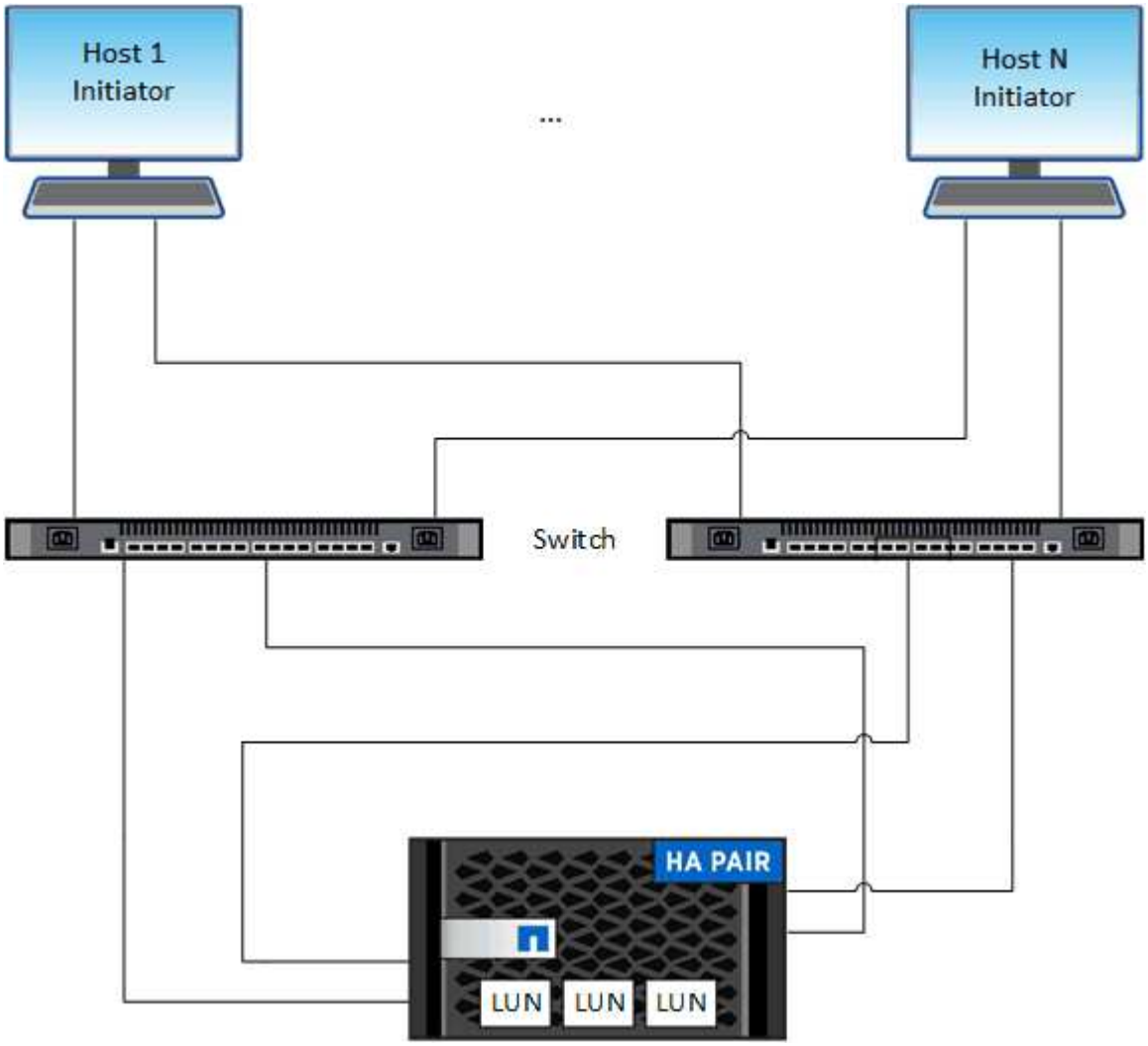
Le contenu de cette section vous explique comment configurer et gérer les environnements SAN avec l'interface de ligne de commande ONTAP et System Manager dans ONTAP 9.7 et versions ultérieures.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous aux rubriques suivantes :

- "Protocole iSCSI"

- "Protocole FC/FCoE"

Vous pouvez utiliser les protocoles iSCSI et FC pour fournir le stockage dans un environnement SAN.



Avec iSCSI et FC, les cibles de stockage sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de bloc standard. Vous créez des LUN, puis les mappez sur des groupes initiateurs. Les groupes initiateurs sont des tableaux des WWPS hôtes FC et des noms de nœuds hôtes iSCSI, et contrôlent les initiateurs auxquels les initiateurs ont accès.

Les cibles FC se connectent au réseau via des commutateurs FC et des adaptateurs côté hôte. Elles sont identifiées par des WWPN (World Wide Port Name). Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet standard (NIC), des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs hôtes principaux dédiés (HBA) et sont identifiées par des noms qualifiés iSCSI (IQN).

Pour en savoir plus

Si vous disposez d'un système de stockage ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 ou ASA A20), reportez-vous au "Documentation du système de stockage ASA r2".

En savoir plus sur les configurations des baies SAN 100 % Flash

Les baies SAN 100 % Flash NetApp sont disponibles à partir de ONTAP 9.7. Les

systèmes ASAS sont des solutions SAN 100 % Flash basées sur les plateformes NetApp éprouvées de AFF.

Les plateformes ASA comprennent les éléments suivants :

- ASA A150
- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

> À partir de ONTAP 9.16.0, une expérience ONTAP simplifiée spécifique aux clients SAN uniquement est disponible sur les systèmes ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 ou ASA A20). Si vous disposez d'un système ASA r2, consultez le "Documentation du système ASA r2".

Les plateformes ASA utilisent une symétrie actif-actif pour les chemins d'accès multiples. Tous les chemins sont optimisés/en mode actif. Ainsi, en cas de basculement de stockage, l'hôte n'a pas besoin d'attendre la transition ALUA des chemins de basculement pour reprendre les E/S. Le délai de basculement est ainsi réduit.

Configurer un ASA

Les baies SAN 100 % Flash (ASA) suivent la même procédure de configuration que les systèmes non ASA.

System Manager vous guide tout au long des procédures nécessaires pour initialiser votre cluster, créer un niveau local, configurer les protocoles et provisionner le stockage de votre ASA.

Commencez avec la configuration de clusters ONTAP.

Utilitaires et paramètres d'hôte ASA

Les paramètres d'hôte pour la configuration des baies SAN 100 % Flash (ASA) sont les mêmes que pour tous les autres hôtes SAN.

Vous pouvez télécharger le "Logiciel NetApp Host Utilities" pour vos hôtes spécifiques sur le site de support.

Méthodes d'identification d'un système ASA

Vous pouvez identifier un système ASA via System Manager ou l'interface de ligne de commandes de ONTAP.

- **Dans le tableau de bord System Manager** : cliquez sur **Cluster > Présentation**, puis sélectionnez le nœud système.

  La **PERSONNALITÉ** s'affiche sous la forme **Baie SAN 100 % Flash**.

- **À partir de l'interface CLI** : entrez le `san config show` commande.

  La valeur « Baie SAN 100 % Flash » est renvoyée pour les systèmes ASA.

Pour en savoir plus, `san config show` consultez le "Référence de commande ONTAP".

Informations associées

- "Rapport technique 4968 : disponibilité et intégrité des données des baies SAN 100 % Flash de NetApp"
- "Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"

Configuration des commutateurs pour FCoE

Vous devez configurer les commutateurs pour FCoE avant que votre service FC ne puisse s'exécuter sur l'infrastructure Ethernet existante.

Avant de commencer

- Votre configuration SAN doit être prise en charge.

  Pour plus d'informations sur les configurations prises en charge, reportez-vous au "Matrice d'interopérabilité NetApp".

- Un adaptateur cible unifié (UTA) doit être installé sur votre système de stockage.

  Si vous utilisez un UTA2, il doit être défini sur `cna` mode.

- Un adaptateur réseau convergé (CNA) doit être installé sur votre hôte.

Étapes

1. Utilisez la documentation de votre commutateur pour configurer vos commutateurs pour FCoE.
2. Vérifiez que les paramètres DCB de chaque nœud du cluster ont été correctement configurés.

   ```
   run -node node1 -command dcb show
   ```

   Les paramètres DCB sont configurés sur le commutateur. Consultez la documentation du commutateur si les paramètres sont incorrects.

3. Vérifiez que la connexion FCoE fonctionne lorsque l'état en ligne du port cible FC est `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   Si l'état en ligne du port FC cible est `false`, consultez la documentation de votre commutateur.

Informations associées

- "Matrice d'interopérabilité NetApp"
- "Rapport technique de NetApp 3800 : guide de déploiement de bout en bout de Fibre Channel over Ethernet (FCoE)"
- "Guides de configuration des logiciels Cisco MDS 9000 NX-OS et SAN-OS"
- "Produits Brocade"

Configuration minimale requise

La configuration des LUN implique la création d'une LUN, la création d'un groupe initiateur et le mappage de celle-ci sur le groupe initiateur. Votre système doit respecter certaines conditions préalables avant de pouvoir configurer vos LUN.

- La matrice d'interopérabilité doit répertorier votre configuration SAN prise en charge.
- Votre environnement SAN doit être conforme aux limites de configuration d'hôtes et de contrôleurs SAN spécifiées dans la "NetApp Hardware Universe" Pour votre version du logiciel ONTAP.
- Une version prise en charge des utilitaires hôtes doit être installée.

  La documentation Host Utilities fournit des informations supplémentaires.

- Vous devez disposer de LIF SAN sur le nœud propriétaire et sur le partenaire HA du nœud propriétaire.

Informations associées

- "Matrice d'interopérabilité NetApp"
- "Configuration de l'hôte SAN ONTAP"
- "Rapport technique de NetApp 4017 : meilleures pratiques liées au SAN Fibre Channel"

Que savoir avant de créer une LUN

Avant de commencer à configurer les LUN sur votre cluster, vous devez consulter les instructions ci-dessous.

Pourquoi la taille réelle des LUN varie légèrement

Concernant la taille de vos LUN, veillez à tenir compte des points suivants.

- Lorsque vous créez une LUN , la taille réelle de celle-ci peut varier légèrement en fonction du type de système d'exploitation de la LUN. Le type de système d'exploitation de LUN ne peut pas être modifié après la création de la LUN.
- Si vous créez une LUN à sa taille maximale, notez que sa taille réelle peut être légèrement inférieure. ONTAP arrondit la limite par excès pour être légèrement inférieur.
- Les métadonnées de chaque LUN requièrent environ 64 Ko d'espace dans l'agrégat contenant. Lorsque vous créez une LUN, vous devez vous assurer que l'agrégat qui contient dispose d'un espace suffisant pour les métadonnées de la LUN. Si l'agrégat ne contient pas assez d'espace pour les métadonnées de la LUN, certains hôtes risquent de ne pas pouvoir accéder à la LUN.

Consignes d'attribution des ID de LUN

En général, l'ID de LUN par défaut commence par 0 et est attribué par incréments de 1 pour chaque LUN mappée supplémentaire. L'hôte associe l'ID de LUN à l'emplacement et au chemin d'accès de la LUN. La plage de numéros d'ID de LUN valides dépend de l'hôte. Pour plus d'informations, consultez la documentation fournie avec vos utilitaires hôtes.

Consignes de mappage des LUN sur les igroups

- Une LUN ne peut être mappée sur un groupe initiateur qu'une seule fois.
- Il est recommandé de mapper une LUN sur un seul initiateur spécifique via le groupe initiateur.

- Vous pouvez ajouter un seul initiateur à plusieurs groupes initiateurs, mais celui-ci ne peut être mappé qu'à une seule LUN.
- Vous ne pouvez pas utiliser le même ID de LUN pour deux LUN mappées sur le même groupe initiateur.
- Vous devez utiliser le même type de protocole pour les groupes initiateurs et les jeux de ports.

Vérifiez et ajoutez votre licence FC ou iSCSI de protocole

Avant de pouvoir activer l'accès aux blocs pour une machine virtuelle de stockage (SVM) avec FC ou iSCSI, vous devez disposer d'une licence. Les licences FC et iSCSI sont incluses dans "ONTAP One".

Exemple 1. Étapes

System Manager

Si vous n'avez pas ONTAP One, vérifiez et ajoutez votre licence FC ou iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

1. Dans System Manager, sélectionnez **Cluster > Paramètres > licences**
2. Si la licence n'est pas répertoriée, sélectionnez + Add et entrez la clé de licence.
3. Sélectionnez **Ajouter**.

CLI

Si vous n'avez pas ONTAP One, vérifiez et ajoutez votre licence FC ou iSCSI via l'interface de ligne de commande ONTAP.

1. Vérifiez que vous disposez d'une licence active pour FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ---------------- ------- --------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Si vous ne disposez pas d'une licence active pour FC ou iSCSI, ajoutez votre code de licence.

```
license add -license-code <your_license_code>
```

Provisionnement du stockage SAN

Cette procédure crée de nouvelles LUN sur une machine virtuelle de stockage existante sur laquelle le protocole FC ou iSCSI est déjà configuré.

Description de la tâche

Cette procédure s'applique aux systèmes FAS, AFF et ASA. Si vous possédez un système ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 ou ASA C30), suivez "procédure à suivre" pour provisionner votre stockage. Les systèmes ASA r2 simplifient l'expérience ONTAP propre aux clients SAN.

Si vous devez créer une nouvelle machine virtuelle de stockage et configurer le protocole FC ou iSCSI, reportez-vous à la section "Configuration d'un SVM pour FC" ou "Configuration d'un SVM pour iSCSI".

Si la licence FC n'est pas activée, les LIFs et les SVM semblent être en ligne, mais le statut opérationnel est arrêté.

Les LUN apparaissent sur votre hôte en tant que périphériques de disque.

> L'accès ALUA (Asymmetric Logical Unit Access) est toujours activé au cours de la création de LUN. Vous ne pouvez pas modifier le paramètre ALUA.

Vous devez utiliser un zoning unique pour toutes les LIFs FC du SVM pour héberger les initiateurs.

Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.

Exemple 2. Étapes

System Manager

Créer des LUN pour fournir du stockage à un hôte SAN à l'aide du protocole FC ou iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour effectuer cette tâche à l'aide de System Manager Classic (disponible avec les versions 9.7 et antérieures), reportez-vous à la section "Configuration iSCSI pour Red Hat Enterprise Linux"

Étapes

1. Installez le approprié "Utilitaires d'hôte SAN" sur votre hôte.
2. Dans System Manager, cliquez sur **stockage > LUN**, puis sur **Ajouter**.
3. Indiquez les informations requises pour la création de la LUN.
4. Vous pouvez cliquer sur **plus d'options** pour effectuer l'une des opérations suivantes, selon votre version de ONTAP.

Option	Disponible à partir de
• Attribuez la politique de QoS aux LUN au lieu du volume parent ◦ **Plus d'options > stockage et optimisation** ◦ Sélectionnez **Performance Service Level**. ◦ Pour appliquer la stratégie QoS à des LUN individuelles au lieu du volume entier, sélectionnez **appliquer ces seuils de performances à chaque LUN**. Par défaut, des limites de performances sont appliquées au niveau du volume.	ONTAP 9.10.1
• Créez un nouveau groupe initiateur à l'aide des groupes initiateurs existants ◦ **Plus d'options > INFORMATIONS SUR L'HÔTE** ◦ Sélectionnez **Nouveau groupe initiateur utilisant des groupes initiateurs** existants. ⓘ Le type de système d'exploitation d'un groupe initiateur contenant d'autres groupes initiateurs ne peut pas être modifié après sa création.	ONTAP 9.9.1
• Ajoutez une description à votre groupe initiateur ou à votre initiateur hôte La description sert d'alias pour le groupe initiateur ou l'initiateur hôte. ◦ **Plus d'options > INFORMATIONS SUR L'HÔTE**	ONTAP 9.9.1

• Créez votre LUN sur un volume existant Par défaut une nouvelle LUN est créée dans un nouveau volume. ◦ **Plus d'options > Ajouter des LUN** ◦ Sélectionnez **groupes de LUN connexes**.	ONTAP 9.9.1
• Désactivez la QoS ou choisissez une règle de QoS personnalisée ◦ **Plus d'options > stockage et optimisation** ◦ Sélectionnez **Performance Service Level**. Dans ONTAP 9.9.1 et versions ultérieures, si vous sélectionnez une stratégie de QoS personnalisée, vous pouvez également sélectionner le placement manuel sur un niveau local spécifié.	ONTAP 9.8

5. Pour FC, désegmentation des commutateurs FC par WWPN. Utilisez une zone par initiateur et incluez tous les ports cibles dans chaque zone.
6. Découvrez les LUN sur votre hôte

   Pour VMware vSphere, utilisez Virtual Storage Console (VSC) pour détecter et initialiser vos LUN.

7. Initialisez les LUN et, éventuellement, créez des systèmes de fichiers.
8. Vérifiez que l'hôte peut écrire et lire les données sur la LUN.

CLI

Créer des LUN afin de fournir le stockage d'un hôte SAN utilisant le protocole FC ou iSCSI avec l'interface de ligne de commande de ONTAP.

1. Vérifiez que vous disposez d'une licence pour FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Si vous ne disposez pas de licence pour FC ou iSCSI, utilisez le `license add` commande.

```
license add -license-code <your_license_code>
```

3. Activer votre service de protocole sur le SVM :

   Pour iSCSI:

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   Pour FC:

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. Créez deux LIF pour les SVM sur chaque nœud :

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   NetApp prend en charge au moins une LIF iSCSI ou FC par nœud pour chaque SVM assurant le service des données. Cependant, deux LIF par nœud sont nécessaires pour assurer la redondance. Pour iSCSI, il est recommandé de configurer au moins deux LIF par nœud dans des réseaux Ethernet distincts.

5. Vérifiez que vos LIF ont été créées et que leur statut opérationnel est `online`:

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. Création de vos LUN :

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   Le nom de LUN ne doit pas dépasser 255 caractères et ne peut pas contenir d'espaces.

   > L'option NVFAIL est automatiquement activée lorsqu'une LUN est créée dans un volume.

7. Création de vos igroups :

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. Mappage de vos LUN sur des igroups :

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Vérifiez que vos LUN sont configurées correctement :

```
lun show -vserver <svm_name>
```

10. En option, "Créez un port défini et associez-le à un groupe initiateur".
11. Suivez les étapes de la documentation de votre hôte pour activer l'accès aux blocs sur vos hôtes spécifiques.
12. Utilisez les utilitaires hôtes pour terminer le mappage FC ou iSCSI et détecter vos LUN sur l'hôte.

Informations associées

- "Présentation de L'administration SAN"
- "Configuration de l'hôte SAN ONTAP"
- "Afficher et gérer les groupes initiateurs SAN dans System Manager"
- "Rapport technique de NetApp 4017 : meilleures pratiques liées au SAN Fibre Channel"

Provisionnement NVMe

Présentation de NVMe

Vous pouvez utiliser le protocole NVMe (non-volatile Memory Express) pour fournir du stockage dans un environnement SAN. Le protocole NVMe est optimisé pour les performances du stockage Solid state.

Pour NVMe, les cibles de stockage sont appelées espaces de noms. Un namespace NVMe est une quantité de stockage non volatile pouvant être formatée dans des blocs logiques et présentée à un hôte comme un périphérique de bloc standard. Vous créez des espaces de noms et des sous-systèmes, puis mappez les espaces de noms aux sous-systèmes, de la même manière que les LUN sont provisionnées et mappées aux igroups pour FC et iSCSI.

Les cibles NVMe sont connectées au réseau via une infrastructure FC standard en utilisant des switchs FC ou une infrastructure TCP standard à l'aide de switchs Ethernet et d'adaptateurs côté hôte.

La prise en charge de NVMe varie selon votre version d'ONTAP. Voir "Prise en charge et limitations de NVMe" pour plus d'informations.

Qu'est-ce que NVMe

Le protocole NVMe (Nonvolatile Memory Express) est un protocole de transport utilisé pour l'accès aux supports de stockage non volatiles.

NVMe over Fabrics (NVMeoF) est une extension définie par la spécification vers NVMe qui permet une communication basée sur NVMe avec des connexions autres que PCIe. Cette interface permet de connecter

des armoires de stockage externes à un serveur.

Conçue pour fournir un accès efficace aux dispositifs de stockage conçus avec une mémoire non volatile, de la technologie Flash aux technologies de mémoire persistante plus performantes. En tant que telle, elle ne présente pas les mêmes limites que les protocoles de stockage conçus pour les disques durs. Les périphériques Flash et Solid State Devices (SSD) sont un type de mémoire non volatile (NVM). NVM est un type de mémoire qui conserve son contenu pendant une coupure de courant. C'est une méthode qui vous permet d'accéder à cette mémoire.

La vitesse, la productivité, le débit et la capacité accrues sont autant d'avantages pour le transfert de données. Caractéristiques spécifiques :

- NVMe est conçu pour accueillir jusqu'à 64 000 files d'attente.

  Chaque file d'attente peut à son tour comporter jusqu'à 64 000 commandes simultanées.

- La technologie NVMe est prise en charge par plusieurs fournisseurs matériels et logiciels
- NMVe est plus productif grâce aux technologies Flash, qui accélèrent les temps de réponse
- NVMe autorise plusieurs requêtes de données pour chaque « demande » envoyée vers le SSD.

  NVMe apporte moins de temps à décoder une « recherche » et n'exige pas de verrouillage des threads dans un programme multithread.

- NVMe prend en charge des fonctionnalités qui empêchent les goulots d'étranglement au niveau du CPU et assure une évolutivité massive au fur et à mesure que les systèmes augmentent.

À propos des espaces de noms NVMe

Un namespace NVMe est une quantité de mémoire non volatile (NVM) pouvant être formatée dans des blocs logiques. Les espaces de noms sont utilisés lorsqu'un serveur virtuel de stockage est configuré avec le protocole NVMe et équivalent de LUN pour les protocoles FC et iSCSI.

Un ou plusieurs espaces de noms sont provisionnés et connectés à un hôte NVMe. Chaque espace de noms peut prendre en charge plusieurs tailles de blocs.

Le protocole NVMe donne accès aux espaces de noms via plusieurs contrôleurs. À l'aide des pilotes NVMe, pris en charge sur la plupart des systèmes d'exploitation, les espaces de noms des disques SSD apparaissent comme des périphériques de bloc standard sur lesquels les systèmes de fichiers et les applications peuvent être déployés sans aucune modification.

Un ID d'espace de noms (NSID) est un identifiant utilisé par un contrôleur pour fournir l'accès à un espace de noms. Lors de la définition du NSID pour un hôte ou un groupe d'hôtes, vous configurez également l'accessibilité à un volume par un hôte. Un bloc logique ne peut être mappé qu'à un seul groupe d'hôtes à la fois et un groupe d'hôtes donné ne possède pas de NSID en double.

À propos des sous-systèmes NVMe

Un sous-système NVMe comprend un ou plusieurs contrôleurs NVMe, des espaces de noms, des ports de sous-système NVM, un support de stockage NVM et une interface entre le contrôleur et le support de stockage NVM. Par défaut, lorsque vous créez un namespace NVMe, ce dernier n'est pas mappé sur un sous-système. Vous pouvez également choisir de mapper un sous-système nouveau ou existant.

Informations associées

- Apprenez à "Provisionner le stockage NVMe" sur les systèmes ASA, AFF et FAS

- Apprenez à "Mapper un namespace NVMe sur un sous-système" sur les systèmes ASA AFF et FAS.
- "Configuration des hôtes SAN et des clients cloud"
- Apprenez à "Provisionnement du stockage SAN" utiliser les systèmes de stockage ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 ou ASA A20).

Exigences des licences NVMe

Une licence est requise pour la prise en charge de NVMe à partir de ONTAP 9.5. Si NVMe est activé dans ONTAP 9.4, une période de grâce de 90 jours est accordée pour l'acquisition de la licence après la mise à niveau vers ONTAP 9.5.

Vous pouvez activer la licence à l'aide de la commande suivante :

```
system license add -license-code NVMe_license_key
```

Configuration, prise en charge et limitations de NVMe

À partir de ONTAP 9.4, le "NVMe (non-volatile Memory Express)" le protocole est disponible pour les environnements SAN. FC-NVMe utilise la même configuration physique et la même pratique de segmentation que les réseaux FC traditionnels. Toutefois, cette méthode permet une plus grande bande passante, une augmentation des IOPS et une latence réduite que le FC-SCSI.

Les limites et la prise en charge de NVMe varient en fonction de votre version d'ONTAP, de votre plateforme et de votre configuration. Pour plus de détails sur votre configuration spécifique, reportez-vous au "Matrice d'interopérabilité NetApp". Pour connaître les limites prises en charge, voir "Hardware Universe".

> Le nombre maximum de nœuds par cluster est disponible dans Hardware Universe sous **mélange de plates-formes pris en charge**.

Configuration

- Vous pouvez configurer votre configuration NVMe à l'aide d'une structure unique ou multistructure.
- Vous devez configurer une LIF de gestion pour chaque SVM prenant en charge SAN.
- L'utilisation de structures de commutateurs FC hétérogènes n'est pas prise en charge, sauf dans le cas de commutateurs lame intégrés.

  Des exceptions spécifiques sont répertoriées sur le "Matrice d'interopérabilité NetApp".

- Les tissus en cascade, à maillage partiel, à maillage complet, à la périphérie du cœur et au directeur sont tous des méthodes standard de connexion des commutateurs FC à un tissu, et toutes sont prises en charge.

  Une structure peut comprendre un ou plusieurs commutateurs et les contrôleurs de stockage peuvent être connectés à plusieurs commutateurs.

Caractéristiques

Les fonctionnalités NVMe suivantes sont prises en charge selon votre version d'ONTAP.

Depuis ONTAP…	NVMe prend en charge
9.17.1	• Accès hôte NVMe/FC et NVMe/TCP de synchronisation active SnapMirror pour les charges de travail VMware. NVMe/TCP avec VMware dépend de la résolution de l'ID de bogue VMware : TR1049746.
9.15.1	• Configurations IP MetroCluster à quatre nœuds sur NVMe/TCP
9.14.1	• Définition de la priorité de l'hôte au niveau du sous-système (QoS au niveau de l'hôte)
9.12.1	• Configurations IP MetroCluster à quatre nœuds sur NVMe/FC • Les configurations MetroCluster ne sont pas prises en charge pour les réseaux NVMe frontaux avant ONTAP 9.12.1. • Les configurations MetroCluster ne sont pas prises en charge sur NVMe/TCP.
9.10.1	Redimensionnement d'un espace de noms
9.9.1	• Coexistence d'espaces de noms et de LUN sur le même volume
9.8	• Coexistence du protocole Les protocoles SCSI, NAS et NVMe peuvent exister sur la même machine virtuelle de stockage (SVM). Avant ONTAP 9.8, NVMe peut être le seul protocole de la SVM.
9.6	• blocs de 512 octets et blocs de 4096 octets pour espaces de noms 4096 est la valeur par défaut. 512 ne doit être utilisé que si le système d'exploitation hôte ne prend pas en charge les blocs de 4096 octets. • Déplacement de volumes avec espaces de noms mappés

9.5	• Basculement/rétablissement d'une paire haute disponibilité multivoie

Protocoles

Les protocoles NVMe suivants sont pris en charge :

Protocole	Depuis ONTAP…	Autorisé par…
TCP	9.10.1	Valeur par défaut
FC	9.4	Valeur par défaut

À partir de ONTAP 9.8, vous pouvez configurer les protocoles SCSI, NAS et NVMe sur la même machine virtuelle de stockage (SVM).
Dans ONTAP 9.7 et les versions antérieures, NVMe est le seul protocole du SVM.

Espaces de noms

Lorsque vous utilisez des espaces de noms NVMe, vous devez connaître les points suivants :

- Pour ONTAP 9.15.1 et les versions antérieures, ONTAP ne prend pas en charge la commande de gestion des datasets NVMe (désallocation) avec NVMe pour la récupération d'espace.
- Vous ne pouvez pas utiliser SnapRestore pour restaurer un espace de noms à partir d'une LUN, ni inversement.
- La garantie d'espace pour les espaces de noms est identique à la garantie d'espace du volume contenant.
- Vous ne pouvez pas créer d'espace de noms sur une transition de volume à partir d'Data ONTAP 7-mode.
- Les espaces de noms ne prennent pas en charge les éléments suivants :
  - Nouvelles appellations
  - Déplacement inter-volume
  - Copie inter-volume
  - Copie à la demande

Restrictions supplémentaires

Les configurations NVMe ne prennent pas en charge les fonctionnalités d'ONTAP suivantes :

- Virtual Storage Console
- Réserves persistantes

Les éléments suivants s'appliquent uniquement aux nœuds exécutant ONTAP 9.4 :

- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Le service NVMe doit être créé avant la création du LIF NVMe.

Informations associées

"Bonnes pratiques pour le SAN moderne"

Configuration d’une VM de stockage pour NVMe

Si vous souhaitez utiliser le protocole NVMe sur un nœud, vous devez configurer votre SVM spécifiquement pour NVMe.

Avant de commencer

Vos adaptateurs FC ou Ethernet doivent prendre en charge NVMe. Les adaptateurs pris en charge sont répertoriés dans le "NetApp Hardware Universe".

Exemple 3. Étapes

System Manager

Configurer une machine virtuelle de stockage pour NVMe avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer NVMe sur une nouvelle machine virtuelle de stockage	Pour configurer NVMe sur une VM de stockage existante
1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**. 2. Entrez un nom pour la machine virtuelle de stockage. 3. Sélectionnez **NVMe** pour le **Protocole d'accès**. 4. Sélectionnez **Activer NVMe/FC** ou **Activer NVMe/TCP** et **Enregistrer**.	1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**. 2. Cliquez sur la VM de stockage que vous souhaitez configurer. 3. Cliquez sur l'onglet **Settings**, puis cliquez sur ⚙ en regard du protocole NVMe. 4. Sélectionnez **Activer NVMe/FC** ou **Activer NVMe/TCP** et **Enregistrer**.

CLI

Configurez une VM de stockage pour NVMe avec l'interface de ligne de commande de ONTAP.

1. Si vous ne souhaitez pas utiliser un SVM existant, créez un :

   ```
   vserver create -vserver <SVM_name>
   ```

   a. Vérifier que le SVM est créé :

   ```
   vserver show
   ```

2. Vérifiez que des adaptateurs compatibles NVMe ou TCP sont installés dans votre cluster :

   Pour NVMe :

   ```
   network fcp adapter show -data-protocols-supported fc-nvme
   ```

   Pour TCP :

   ```
   network port show
   ```

   Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

3. Si vous exécutez ONTAP 9.7 ou version antérieure, supprimez tous les protocoles du SVM :

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

Depuis la version ONTAP 9.8, il n'est pas nécessaire de supprimer d'autres protocoles lors de l'ajout de NVMe.

4. Ajoutez le protocole NVMe au SVM :

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Si vous exécutez ONTAP 9.7 ou une version antérieure, vérifiez que NVMe est le seul protocole autorisé sur le SVM :

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe doit être le seul protocole affiché sous le `allowed protocols` colonne.

6. Créez le service NVMe :

```
vserver nvme create -vserver <SVM_name>
```

7. Vérifiez que le service NVMe a été créé :

```
vserver nvme show -vserver <SVM_name>
```

Celui `Administrative Status` de la SVM doit être répertorié comme `up`. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".

8. Créez une LIF NVMe/FC :
   - Pour ONTAP 9.9.1 ou version antérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - Pour ONTAP 9.10.1 ou version ultérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- Pour ONTAP 9.10.1 ou version ultérieure, TCP :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. Créer une LIF NVMe/FC sur le nœud partenaire HA :
   - Pour ONTAP 9.9.1 ou version antérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - Pour ONTAP 9.10.1 ou version ultérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

   - Pour ONTAP 9.10.1 ou version ultérieure, TCP :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. Vérifiez que les LIF NVMe/FC ont été créées :

```
network interface show -vserver <SVM_name>
```

11. Création de volumes sur le même nœud que la LIF :

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Si un message d'avertissement relatif à la stratégie d'efficacité automatique s'affiche, il peut être ignoré en toute sécurité.

Provisionner le stockage NVMe

Suivez ces étapes pour créer des espaces de noms et provisionner du stockage pour tout hôte NVMe pris en charge sur une machine virtuelle de stockage existante.

Description de la tâche

Cette procédure s'applique aux systèmes FAS, AFF et ASA. Si vous possédez un système ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 ou ASA C30), suivez "procédure à suivre" pour provisionner votre stockage. Les systèmes ASA r2 simplifient l'expérience ONTAP propre aux clients SAN.

Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.

Avant de commencer

Votre VM de stockage doit être configurée pour NVME, et votre transport FC ou TCP doit déjà être configuré.

System Manager

En utilisant ONTAP System Manager (9.7 et versions ultérieures), créez des espaces de noms pour fournir un stockage à l'aide du protocole NVMe.

Étapes

1. Dans System Manager, cliquez sur **stockage > espaces de noms NVMe**, puis sur **Ajouter**.

   Si vous devez créer un nouveau sous-système, cliquez sur **plus d'options**.

2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que vous souhaitez désactiver la qualité de service ou choisir une stratégie de qualité de service personnalisée, cliquez sur **plus d'options**, puis, sous **stockage et optimisation**, sélectionnez **niveau de service de performances**.
3. Segmenter vos commutateurs FC par WWPN. Utilisez une zone par initiateur et incluez tous les ports cibles dans chaque zone.
4. Sur votre hôte, découvrez les nouveaux espaces de noms.
5. Initialiser l'espace de noms et le formater avec un système de fichiers.
6. Vérifiez que votre hôte peut écrire et lire les données sur le namespace.

CLI

En utilisant l'interface de ligne de commande d'ONTAP, créez des espaces de noms pour fournir le stockage à l'aide du protocole NVMe.

Cette procédure crée un namespace et un sous-système NVMe sur une VM de stockage existante déjà configurée pour le protocole NVMe, puis mappe l'espace de noms sur le sous-système pour permettre l'accès aux données de votre système hôte.

Si vous devez configurer la machine virtuelle de stockage pour NVMe, reportez-vous à la section "Configuration d'un SVM pour NVMe".

Étapes

1. Vérifier que le SVM est configuré pour NVMe :

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` doit s'afficher sous le `allowed-protocols` colonne.

2. Créez le namespace NVMe :

   > Le volume que vous référencez avec le `-path` paramètre doit déjà exister ou vous devez en créer un avant d'exécuter cette commande.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. Créez le sous-système NVMe :

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

Le nom du sous-système NVMe est sensible à la casse. Ils doivent comporter entre 1 et 96 caractères. Les caractères spéciaux sont autorisés.

4. Vérifiez que le sous-système a été créé :

```
vserver nvme subsystem show -vserver <svm_name>
```

Le `nvme` le sous-système doit s'afficher sous `Subsystem` colonne.

5. Obtenez le NQN de l'hôte.
6. Ajoutez le NQN hôte au sous-système :

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mapper l'espace de noms au sous-système :

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

Un espace de noms ne peut être mappé qu'à un seul sous-système.

8. Vérifiez que l'espace de noms est mappé sur le sous-système :

```
vserver nvme namespace show -vserver <svm_name> -instance
```

Le sous-système doit être répertorié comme `Attached subsystem`.

Mappez un namespace NVMe à un sous-système

Le mappage d'un namespace NVMe sur un sous-système permet l'accès aux données depuis votre hôte. Vous pouvez mapper un namespace NVMe à un sous-système lors du provisionnement du stockage ou le faire une fois celui-ci provisionné.

À partir d' ONTAP 9.17.1, si vous utilisez une configuration SnapMirror Active Sync, vous pouvez ajouter une SVM à un hôte en tant que serveur virtuel proximal lors de l'ajout de l'hôte à un sous-système NVMe. Les chemins optimisés pour un espace de noms dans un sous-système NVMe sont publiés sur un hôte uniquement à partir de la SVM configurée comme serveur virtuel proximal.

À partir de ONTAP 9.14.1, vous pouvez hiérarchiser l'allocation des ressources pour des hôtes spécifiques.

Par défaut, lorsqu'un hôte est ajouté au sous-système NVMe, sa priorité est donnée. Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour modifier manuellement la priorité par défaut, de normal à élevée. Les hôtes affectés à une priorité élevée reçoivent un nombre de files d'attente d'E/S et des profondeurs de files d'attente plus importants.

> Si vous souhaitez donner une priorité élevée à un hôte ajouté à un sous-système dans ONTAP 9.13.1 ou une version antérieure, vous pouvez le faire modifiez la priorité de l'hôte.

Avant de commencer

Votre espace de noms et votre sous-système doivent déjà être créés. Si vous devez créer un espace de noms et un sous-système, reportez-vous à la section "Provisionner le stockage NVMe".

Cartographier un espace de noms NVMe

Étapes

1. Obtenez le NQN de l'hôte.
2. Ajoutez le NQN hôte au sous-système :

   ```
   vserver nvme subsystem host add -vserver <SVM_name> -subsystem
   <subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
   ```

   Si vous souhaitez modifier la priorité par défaut de l'hôte de normal à élevé, utilisez l' `-priority high`option. Cette option est disponible à partir de ONTAP 9.14.1. Pour en savoir plus, `vserver nvme subsystem host add` consultez le "Référence de commande ONTAP".

   Si vous souhaitez ajouter un SVM en tant que `proximal-vserver` à un hôte lors de l'ajout de l'hôte à un sous-système NVMe dans une configuration de synchronisation active SnapMirror , vous pouvez utiliser le `-proximal-vservers` Option. Cette option est disponible à partir d' ONTAP 9.17.1. Vous pouvez ajouter la SVM source ou de destination, ou les deux. La SVM dans laquelle vous exécutez cette commande est celle par défaut.

3. Mapper l'espace de noms au sous-système :

   ```
   vserver nvme subsystem map add -vserver <SVM_name> -subsystem
   <subsystem_name> -path <path>
   ```

   Un espace de noms ne peut être mappé qu'à un seul sous-système. Pour en savoir plus, `vserver nvme subsystem map add` consultez le "Référence de commande ONTAP".

4. Vérifiez que l'espace de noms est mappé sur le sous-système :

   ```
   vserver nvme namespace show -vserver <SVM_name> -instance
   ```

   Le sous-système doit être répertorié comme `Attached subsystem` . Pour en savoir plus, `vserver nvme namespace show` consultez le "Référence de commande ONTAP".

Gérer les LUN

Modifiez la « policy group » QoS de la LUN

À partir d'ONTAP 9.10.1, vous pouvez utiliser System Manager pour attribuer ou supprimer des stratégies de qualité de service (QoS) sur plusieurs LUN en même temps.

> Si la politique de QoS est attribuée au niveau du volume, elle doit être modifiée au niveau du volume. Vous pouvez modifier la règle de qualité de services au niveau des LUN uniquement s'il a été initialement attribué au niveau des LUN.

Étapes

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Sélectionnez la ou les LUN à modifier.

   Si vous modifiez plusieurs LUN à la fois, les LUN doivent appartenir au même SVM (Storage Virtual machine). Si vous sélectionnez des LUN qui n'appartiennent pas au même SVM, l'option de modification du QoS Policy Group n'est pas affichée.

3. Cliquez sur **plus** et sélectionnez **Modifier groupe de stratégies QoS**.

Convertir une LUN en espace de nom

Depuis ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes de ONTAP pour convertir un LUN existant en espace de noms NVMe, sans déplacement des données.

Avant de commencer

- La LUN spécifiée ne doit pas disposer d'aucun mappage existant sur un groupe initiateur.
- Le LUN ne doit pas se trouver dans un SVM configuré par MetroCluster ni dans une relation de synchronisation active SnapMirror.
- La LUN ne doit pas être un terminal de protocole ni être liée à un terminal de protocole.
- La LUN ne doit pas contenir de préfixe et/ou de flux de suffixe non nul.
- La LUN ne doit pas faire partie d'un snapshot ou du côté destination d'une relation SnapMirror en tant que LUN en lecture seule.

Étape

1. Convertir une LUN en namespace NVMe :

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

Mettez une LUN hors ligne

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour mettre les LUN hors ligne. Avant ONTAP 9.10.1, vous devez utiliser l'interface de ligne de commandes de ONTAP pour mettre les LUN hors ligne.

System Manager

Étapes

1. Dans System Manager, cliquez sur **stockage> LUN**.
2. Mettre une ou plusieurs LUN hors ligne

Si vous voulez…	Faites cela…
Mettez une LUN hors ligne	En regard du nom de la LUN, cliquez sur ⋮ et sélectionnez **mettre hors ligne**.
Mettre plusieurs LUN hors ligne	1. Sélectionnez les LUN que vous souhaitez mettre hors ligne. 2. Cliquez sur **plus** et sélectionnez **mettre hors ligne**.

CLI

Vous ne pouvez mettre une LUN hors ligne qu'à la fois lorsque vous utilisez l'interface de ligne de commandes.

Étape

1. Mettre la LUN hors ligne :

```
lun offline <lun_name> -vserver <SVM_name>
```

Redimensionner une LUN dans ONTAP

Vous pouvez augmenter ou réduire la taille d'une LUN.

Description de la tâche

Cette procédure s'applique aux systèmes FAS, AFF et ASA. Si vous possédez un système ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 ou ASA C30), suivez "procédure à suivre" pour augmenter la taille d'une unité de stockage. Les systèmes ASA r2 simplifient l'expérience ONTAP propre aux clients SAN.

ⓘ Les LUN Solaris ne peuvent pas être redimensionnées.

Augmentez la taille d'une LUN

La taille à laquelle vous pouvez augmenter le nombre de LUN dépend de votre version de ONTAP.

Version ONTAP	Taille maximale de LUN
ONTAP 9.12.1P2 et versions ultérieures	128 To pour les plateformes AFF, FAS et ASA

ONTAP 9.8 et versions ultérieures	• 128 To pour les plateformes de baies SAN 100 % Flash (ASA) • 16 To pour les plateformes non ASA
ONTAP 9.5, 9.6, 9.7	16 TO
ONTAP 9.4 ou version antérieure	10 fois la taille de LUN d'origine, mais pas supérieure à 16 To, ce qui correspond à la taille de LUN maximale. Par exemple, si vous créez une LUN de 100 Go, vous ne pouvez la faire évoluer qu'à 1,000 Go. La taille maximale réelle de la LUN peut ne pas être exactement 16 To. ONTAP arrondit la limite par excès pour être légèrement inférieur.

Il n'est pas nécessaire de mettre la LUN hors ligne pour augmenter la taille. Toutefois, une fois la taille augmentée, vous devez relancer une nouvelle analyse du LUN sur l'hôte pour que l'hôte reconnaisse la modification de taille.

Exemple 4. Étapes

System Manager

Augmentez la taille d'une LUN avec ONTAP System Manager (9.7 et versions ultérieures).

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Cliquez sur ⋮ et sélectionnez **Modifier**.
3. Sous **stockage et optimisation**, augmentez la taille du LUN et **Enregistrer**.

CLI

Augmentez la taille d'une LUN à l'aide de l'interface de ligne de commandes de ONTAP.

1. Augmenter la taille de la LUN :

   ```
   lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size>
   ```

   Pour en savoir plus, `lun resize` consultez le "Référence de commande ONTAP".

2. Vérifiez que la taille de LUN augmente :

   ```
   lun show -vserver <SVM_name>
   ```

Les opérations de ONTAP arrondissez la taille maximale réelle de la LUN. Celle-ci est donc légèrement inférieure à la valeur attendue. Par ailleurs, la taille de LUN réelle peut varier légèrement en fonction du type de système d'exploitation de la LUN. Pour obtenir la valeur redimensionnée exacte, exécutez les commandes

suivantes en mode avancé :

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+
Pour en savoir plus, `lun show` consultez le "Référence de commande ONTAP".

1. Relancez l'analyse de la LUN sur l'hôte.
2. Suivez la documentation de votre hôte pour que la taille de LUN créée soit visible par le système de fichiers hôte.

Réduisez la taille d'une LUN

Avant de réduire la taille d'une LUN, l'hôte doit migrer les blocs contenant les données de LUN vers le limite de la taille de LUN inférieure. Vous devez utiliser un outil tel que SnapCenter pour vous assurer que la LUN est correctement réduite sans tronquer les blocs contenant des données de LUN. Il est déconseillé de réduire manuellement la taille de la LUN.

Une fois que vous avez réduit la taille de la LUN, ONTAP informe automatiquement l'initiateur que sa taille a diminué. Toutefois, des étapes supplémentaires peuvent être nécessaires sur votre hôte pour reconnaître la nouvelle taille de LUN. Consultez la documentation de votre hôte pour obtenir des informations spécifiques sur la diminution de la taille de la structure de fichiers hôte.

Déplacer une LUN

Vous pouvez déplacer une LUN entre des volumes au sein d'un SVM, mais il n'est pas possible de déplacer une LUN entre ces SVM. Les LUN déplacées entre les volumes d'un SVM sont immédiatement déplacés et sans perte de connectivité.

Avant de commencer

Si votre LUN utilise la fonction de mappage de LUN sélectif (SLM), vous devez "Modifiez la liste des nœuds de création de rapports SLM" Pour inclure le nœud de destination et son partenaire haute disponibilité avant de déplacer la LUN.

Description de la tâche

Les fonctionnalités d'efficacité du stockage, telles que la déduplication, la compression et la compaction, ne sont pas conservées pendant un déplacement de LUN. Elles doivent être de nouveau appliquées une fois le déplacement de LUN terminé.

La protection des données via des snapshots s'effectue au niveau des volumes. Par conséquent, lorsque vous déplacez une LUN, elle tombe sous le schéma de protection des données du volume de destination. Si aucun snapshot n'est établi pour le volume de destination, les snapshots de la LUN ne sont pas créés. Par ailleurs, tous les snapshots de la LUN restent dans le volume d'origine jusqu'à ce que ces snapshots soient supprimés.

Vous ne pouvez pas déplacer une LUN vers les volumes suivants :

- Volume de destination SnapMirror
- Root volume du SVM

Vous ne pouvez pas déplacer les types de LUN suivants :

- LUN créée à partir d'un fichier
- LUN en état NVFail
- LUN faisant partie d'une relation de partage de charge
- LUN de classe terminal-protocole

Lorsque les nœuds d'un cluster utilisent des versions ONTAP différentes, vous ne pouvez déplacer un LUN entre des volumes de différents nœuds que si la source utilise une version ultérieure à la destination. Par exemple, si le nœud du volume source utilise ONTAP 9.15.1 et celui du volume de destination ONTAP 9.16.1, vous ne pouvez pas déplacer le LUN. Vous pouvez déplacer des LUN entre des volumes de nœuds utilisant la même version ONTAP .

> Pour les LUN Solaris de type os qui sont de 1 To ou plus, l'hôte peut connaître un délai d'expiration lors du déplacement de LUN. Pour ce type de LUN, vous devez démonter la LUN avant d'initier la migration.

Exemple 5. Étapes

System Manager

Déplacez une LUN avec ONTAP System Manager (9.7 et versions ultérieures).

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour créer un volume lorsque vous déplacez un seul LUN. Dans ONTAP 9.8 et 9.9.1, le volume vers lequel vous déplacez le LUN doit exister avant de lancer le déplacement de LUN.

Étapes

1. Dans System Manager, cliquez sur **stockage> LUN**.
2. Cliquez avec le bouton droit de la souris sur la LUN à déplacer, puis cliquez sur ⋮ et sélectionnez **déplacer LUN**.

   Dans ONTAP 9.10.1, sélectionnez pour déplacer le LUN vers **un volume existant** ou vers **Nouveau volume**.

   Si vous choisissez de créer un nouveau volume, indiquez les spécifications du volume.

3. Cliquez sur **déplacer**.

CLI

Déplacez une LUN avec l'interface de ligne de commandes de ONTAP.

1. Déplacer la LUN :

   ```
   lun move start
   ```

   Pendant une très brève période, la LUN est visible à la fois sur le volume d'origine et sur le volume de destination. Ceci est prévu et résolu à la fin de la transition.

2. Suivre l'état du déplacement et vérifier que l'opération a bien été effectuée :

   ```
   lun move show
   ```

Informations associées

- "Mappage de LUN sélectif"

Supprimer les LUN

Vous pouvez supprimer une LUN d'un serveur virtuel de stockage (SVM) si vous n'avez plus besoin de la LUN.

Avant de commencer

Pour que vous puissiez le supprimer, vous devez annuler le mappage de la LUN sur son groupe initiateur.

Étapes

1. Vérifiez que l'application ou l'hôte n'utilise pas la LUN.
2. Annulez le mappage de la LUN du groupe initiateur :

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. Supprimer la LUN :

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Vérifiez que vous avez supprimé la LUN :

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

Que devez-vous savoir avant de copier des LUN

Avant de copier une LUN, vous devez connaître certaines informations.

Les administrateurs de cluster peuvent copier une LUN sur des serveurs virtuels de stockage (SVM) au sein du cluster à l'aide de `lun copy` commande. Les administrateurs de cluster doivent établir la relation de peering de la machine virtuelle de stockage (SVM) à l'aide de `vserver peer create` Commande avant l'exécution d'une opération de copie de LUN inter-SVM. Il doit y avoir suffisamment d'espace dans le volume source pour un clone SIS.

Les LUN des snapshots peuvent être utilisées comme LUN source pour la `lun copy` commande. Lorsque vous copiez une LUN à l'aide de `lun copy` la commande, la copie de LUN est immédiatement disponible pour l'accès en lecture et en écriture. La LUN source reste inchangée par la création d'une copie LUN. La LUN source et la copie de LUN existent tous deux en tant que LUN uniques avec différents numéros de série de LUN. Les modifications apportées à la LUN source ne sont pas reflétées dans la copie de LUN, et les modifications apportées à cette copie ne sont pas prises en compte dans la LUN source. Le mappage de LUN de la LUN source n'est pas copié sur la nouvelle LUN ; la copie de LUN doit être mappée.

La protection des données via des snapshots s'effectue au niveau des volumes. Par conséquent, si vous copiez une LUN vers un volume différent du volume de la LUN source, celle-ci se trouve sous le schéma de protection des données du volume de destination. Si aucun snapshot n'est défini pour le volume de destination, les snapshots ne sont pas créés pour la copie de LUN.

La copie des LUN s'effectue sans interruption.

Vous ne pouvez pas copier les types de LUN suivants :

- LUN créée à partir d'un fichier
- LUN en état NVFAIL
- LUN faisant partie d'une relation de partage de charge
- LUN de classe terminal-protocole

Pour en savoir plus, `lun copy` consultez le "Référence de commande ONTAP".

Examen de l'espace configuré et utilisé d'une LUN

En sachant l'espace configuré et l'espace réel utilisé pour vos LUN, vous pouvez déterminer la quantité d'espace que vous pouvez récupérer lors de la récupération de l'espace, la quantité d'espace réservé contenant les données, et la taille totale configurée par rapport à la taille réelle utilisée pour une LUN.

Étape

1. Afficher l'espace configuré et l'espace réel utilisé par une LUN :

   ```
   lun show
   ```

   L'exemple suivant montre l'espace configuré par rapport à l'espace réel utilisé par les LUN dans la machine virtuelle de stockage vs3 (SVM) :

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- -----------------       ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

   Pour en savoir plus, `lun show` consultez le "Référence de commande ONTAP".

Contrôlez et surveillez les performances d'E/S des LUN grâce à la QoS de stockage

Vous pouvez contrôler les performances des entrées/sorties (E/S) des LUN en affectant des LUN aux groupes de règles de QoS de stockage. Vous pouvez contrôler les performances d'E/S pour permettre aux workloads d'atteindre des objectifs de performance spécifiques ou de limiter les workloads qui ont un impact négatif sur d'autres workloads.

Description de la tâche

Les groupes de règles appliquent une limite de débit maximal (par exemple, 100 Mo/s). Vous pouvez créer un groupe de règles sans spécifier un débit maximal, ce qui vous permet de contrôler les performances avant de contrôler le workload.

Vous pouvez également attribuer des SVM (Storage Virtual machines) avec des volumes FlexVol et des LUN à des groupes de règles.

Prenez en compte les exigences suivantes concernant l'assignation d'une LUN à un « policy group » :

- La LUN doit être contenue par le SVM auquel appartient le « policy group ».

  Vous spécifiez la SVM lors de la création de la « policy group ».

- Si vous attribuez une LUN à une « policy group » alors vous ne pouvez pas attribuer le volume ou SVM contenant la LUN à une « policy group ».

Pour plus d'informations sur l'utilisation de la QoS du stockage, consultez le "Référence d'administration du système".

Étapes

1. Utilisez le `qos policy-group create` commande pour créer une « policy group ».

   Pour en savoir plus, `qos policy-group create` consultez le "Référence de commande ONTAP".

2. Utilisez le `lun create` commande ou le `lun modify` commande avec `-qos-policy-group` Paramètre permettant d'affecter une LUN à une « policy group ».

   Pour en savoir plus, `lun` consultez le "Référence de commande ONTAP".

3. Utilisez le `qos statistics` commandes pour afficher les données de performances.
4. Si nécessaire, utiliser l' `qos policy-group modify` commande pour ajuster la limite de débit maximale du groupe de règles.

   Pour en savoir plus, `qos policy-group modify` consultez le "Référence de commande ONTAP".

Outils disponibles pour surveiller efficacement vos LUN

Des outils sont disponibles pour vous aider à contrôler efficacement vos LUN et à éviter un manque d'espace.

- Active IQ Unified Manager est un outil gratuit qui vous permet de gérer tout le stockage sur tous les clusters de votre environnement.
- System Manager est une interface utilisateur graphique intégrée à ONTAP qui vous permet de gérer manuellement les besoins en stockage au niveau du cluster.
- OnCommand Insight offre une vue unique de l'infrastructure de stockage et vous permet de configurer la surveillance automatique, les alertes et le reporting lorsque vos LUN, volumes et agrégats manquent d'espace de stockage.

Capacités et restrictions des LUN migrées

Dans un environnement SAN, une interruption de service est nécessaire lors de la transition d'un volume 7-mode vers ONTAP. Vous devez arrêter vos hôtes pour terminer la transition. Une fois la transition terminée, vous devez mettre à jour vos configurations hôte pour pouvoir commencer à transférer des données dans ONTAP

Vous devez planifier une fenêtre de maintenance au cours de laquelle vous pouvez arrêter vos hôtes et terminer la transition.

Certaines fonctionnalités et restrictions ont un impact sur la gestion des LUN depuis Data ONTAP 7-mode vers ONTAP.

Vous pouvez faire ce qui suit avec les LUN migrées :

- Affichez la LUN à l'aide de `lun show` commande
- Affichez l'inventaire des LUN migrées depuis le volume 7-mode à l'aide de la `transition 7-mode show` commande
- Restaurez un volume à partir d'un snapshot 7-mode

  La restauration des transitions de volume toutes les LUN capturées dans le snapshot

- Restaurer une LUN unique à partir d'un snapshot 7-mode à l'aide de la `snapshot restore-file` commande
- Créer un clone d'une LUN dans un snapshot 7-mode
- Restaurez une plage de blocs à partir d'une LUN capturée dans un snapshot 7-mode
- Créez une FlexClone du volume à l'aide d'un snapshot 7-mode

Vous ne pouvez pas faire ce qui suit avec les LUN migrées :

- Accédez aux clones LUN sauvegardés par copie Snapshot et capturés dans le volume

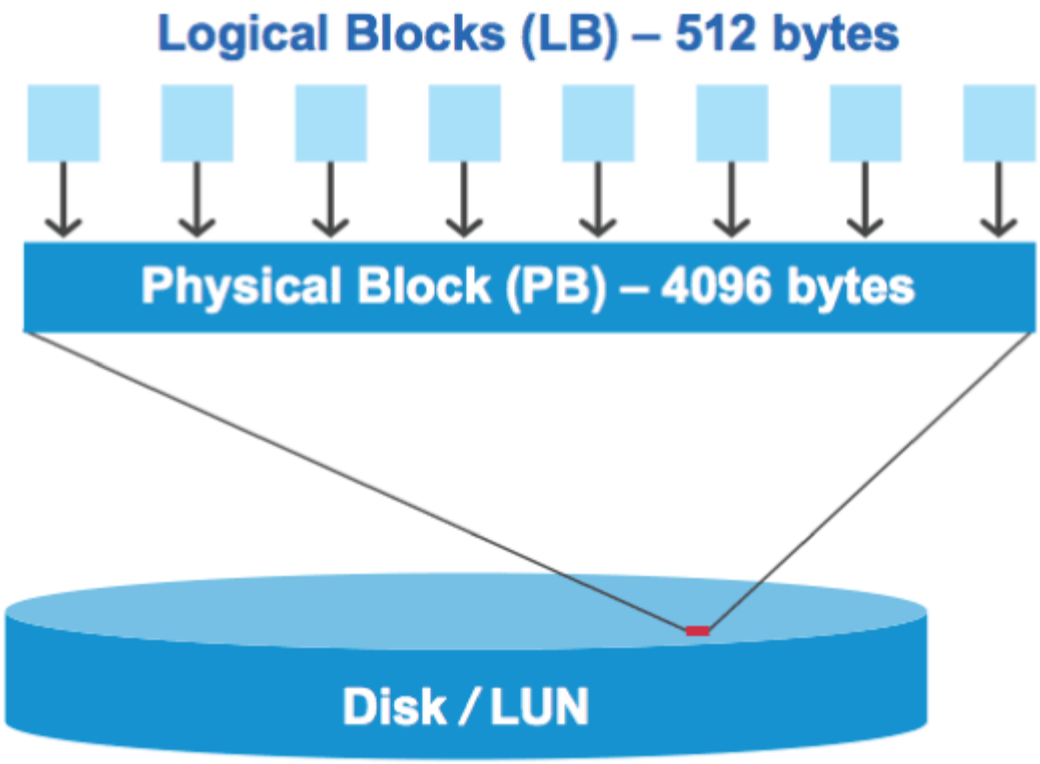
Informations associées

- "Transition basée sur la copie"
- "affichage de la lun"

Aperçu des défauts d'alignement des E/S sur les LUN correctement alignées

ONTAP peut signaler des problèmes d'alignement des E/S sur les LUN correctement alignées. En général, ces avertissements relatifs au mauvais alignement peuvent être ignorés tant que vous êtes sûr que votre LUN est correctement provisionnée et que votre table de partitionnement est correcte.

Les LUN et les disques durs fournissent tous deux un stockage sous forme de blocs. Étant donné que la taille de bloc des disques de l'hôte est de 512 octets, les LUN présentent des blocs de cette taille à l'hôte tout en utilisant des blocs de 4 Ko plus volumineux pour stocker les données. Le bloc de données de 512 octets utilisé par l'hôte est appelé bloc logique. Le bloc de données de 4 Ko utilisé par le LUN pour stocker les données est appelé bloc physique. Cela signifie qu'il y a huit blocs logiques de 512 octets dans chaque bloc physique de 4 Ko.



Le système d'exploitation hôte peut lancer une opération de lecture ou d'écriture d'E/S sur n'importe quel bloc logique. Les opérations d'E/S n'sont considérées comme alignées que lorsqu'elles commencent au premier bloc logique du bloc physique. Si une opération d'E/S commence au démarrage d'un bloc logique qui n'est pas toujours le début d'un bloc physique, les E/S sont considérées comme mal alignées. ONTAP détecte automatiquement l'alignement incorrect et le signale sur le LUN. Toutefois, l'alignement incorrect des E/S n'entraîne pas nécessairement l'alignement incorrect de la LUN. Il est possible de signalement des E/S mal alignées sur les LUN correctement alignées.

Si vous avez besoin d'une enquête plus approfondie, consultez l'article de la base de connaissances "Comment identifier les E/S non alignées sur les LUN ?"

Pour plus d'informations sur les outils de correction des problèmes d'alignement, reportez-vous à la documentation suivante : +

- "Utilitaires d'hôtes unifiés Windows 7.1"
- "Provisionnez la documentation sur le stockage SAN"

Assurez l'alignement des E/S à l'aide des types de systèmes d'exploitation LUN

Pour ONTAP 9.7 ou version antérieure, vous devez utiliser le LUN ONTAP recommandé `ostype` Valeur qui correspond le mieux à votre système d'exploitation pour aligner les E/S avec le schéma de partitionnement du système d'exploitation.

Le schéma de partition utilisé par le système d'exploitation hôte constitue un facteur important de désalignement des E/S. Une LUN ONTAP `ostype` les valeurs utilisent un décalage spécial appelé « préfixe » pour permettre l'alignement du schéma de partitionnement par défaut utilisé par le système d'exploitation hôte.

> Dans certains cas, une table de partitionnement personnalisée peut être nécessaire pour atteindre l'alignement E/S. Cependant, pour `ostype` valeurs dont la valeur « préfixe » est supérieure à `0`, Une partition personnalisée peut créer des E/S mal alignées

Pour plus d'informations sur les LUN provisionnées dans ONTAP 9.7 ou une version antérieure, consultez l'article de la base de connaissances "Comment identifier les E/S non alignées sur les LUN".

> Par défaut, les nouvelles LUN provisionnées dans ONTAP 9.8 ou version ultérieure ont un préfixe et un suffixe de taille zéro pour tous les types de LUN OS. Par défaut, les E/S doivent être alignées sur le système d'exploitation hôte pris en charge.

Considérations spéciales d'alignement des E/S pour Linux

Les distributions Linux offrent de nombreuses façons d'utiliser un LUN, notamment en tant que périphériques bruts pour bases de données, divers gestionnaires de volumes et systèmes de fichiers. Il n'est pas nécessaire de créer des partitions sur un LUN lorsqu'il est utilisé en tant que périphérique brut ou en tant que volume physique dans un volume logique.

Pour RHEL 5 et versions antérieures et SLES 10 et versions antérieures, si le LUN doit être utilisé sans gestionnaire de volumes, vous devez partitionner le LUN pour avoir une partition qui commence à un décalage aligné, ce qui est un secteur qui est un multiple de huit blocs logiques.

Considérations spéciales relatives à l'alignement des E/S pour les LUN Solaris

Vous devez tenir compte de divers facteurs pour déterminer si vous devez utiliser le `solaris` otapez ou le `solaris_efi` ostype.

Voir la "Solaris Host Utilities - Guide d'installation et d'administration" pour des informations détaillées.

Les LUN de démarrage ESX indiquent un mauvais alignement

Les LUN utilisées comme LUN de démarrage ESX sont généralement signalées par ONTAP comme étant mal alignées. ESX crée plusieurs partitions sur la LUN de démarrage, ce qui complique particulièrement l'alignement. Les LUN de démarrage ESX mal alignées ne sont généralement pas problématiques de performances, car la quantité totale d'E/S mal alignées est faible. Supposant que la LUN ait été correctement provisionnée avec VMware `ostype`, aucune action n'est nécessaire.

Informations associées

"Alignement des partitions/disques du système de fichiers des machines virtuelles invité pour VMware vSphere, les autres environnements virtuels et les systèmes de stockage NetApp"

Méthodes pour résoudre les problèmes lorsque les LUN sont mises hors ligne

Lorsqu'aucun espace n'est disponible pour les écritures, les LUN sont mises hors ligne pour préserver l'intégrité des données. Les LUN peuvent manquer d'espace et les mettre hors ligne pour diverses raisons, et il existe plusieurs façons de résoudre le problème.

Si…	Vous pouvez…
L'agrégat est plein	• Ajouter des disques. • Utilisez le `volume modify` commande pour réduire un volume qui dispose d'un espace disponible. • Si vous disposez de volumes Space-Guarantee qui disposent d'espace disponible, définissez la garantie d'espace de volume sur `none` avec le `volume modify` commande.
Le volume est plein, mais l'agrégat contenant est disponible	• Pour les volumes garantis par espace, utilisez `volume modify` commande pour augmenter la taille du volume. • Pour les volumes à provisionnement fin, utilisez le `volume modify` commande pour augmenter la taille maximale du volume. Si la croissance automatique de volume n'est pas activée, utiliser `volume modify -autogrow -mode` pour l'activer. • Supprimez manuellement les snapshots à l'aide de la `volume snapshot delete` commande ou utilisez la `volume snapshot autodelete modify` commande pour supprimer automatiquement les snapshots.

Informations associées

"Gestion des disques et des niveaux locaux (agrégat)"

"Gestion du stockage logique"

Dépanner les LUN iSCSI non visibles sur l'hôte

Les LUN iSCSI apparaissent en tant que disques locaux vers l'hôte. Si les LUN du système de stockage ne sont pas disponibles en tant que disques sur l'hôte, vérifiez les paramètres de configuration.

Paramètre de configuration	Que faire
Câblage	Vérifiez que les câbles entre l'hôte et le système de stockage sont correctement connectés.

Paramètre de configuration	Que faire
Connectivité réseau	Vérifiez que la connectivité TCP/IP est présente entre l'hôte et le système de stockage. • À partir de la ligne de commande du système de stockage, envoyez une requête ping aux interfaces hôtes utilisées pour iSCSI : `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • À partir de la ligne de commande de l'hôte, envoyez une requête ping aux interfaces du système de stockage utilisées pour iSCSI : `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*
Configuration minimale requise	Vérifiez que les composants de votre configuration sont qualifiés. Vérifiez également que vous disposez du niveau de service pack du système d'exploitation hôte, de la version de l'initiateur, de la version de ONTAP et des autres exigences système appropriées. La matrice d'interopérabilité présente les conditions système les plus récentes.
Trames Jumbo	Si vous utilisez des trames Jumbo dans votre configuration, vérifiez que ces trames jumbo sont activées sur tous les périphériques du chemin réseau : la carte réseau Ethernet hôte, le système de stockage et tous les commutateurs.
État du service iSCSI	Vérifiez que le service iSCSI est sous licence et démarré sur le système de stockage.
Connexion à l'initiateur	Vérifiez que l'initiateur est connecté au système de stockage. Si le `iscsi initiator show` le résultat de la commande affiche qu'aucun initiateur n'est connecté, vérifiez la configuration de l'initiateur sur l'hôte. Vérifiez également que le système de stockage est configuré comme cible de l'initiateur.
Noms des nœuds iSCSI (IQN)	Vérifiez que vous utilisez les noms de nœud d'initiateur corrects dans la configuration de votre groupe initiateur. Sur l'hôte, vous pouvez utiliser les outils et les commandes de l'initiateur pour afficher le nom du nœud initiateur. Les noms de nœud initiateur configurés dans le groupe initiateur et sur l'hôte doivent correspondre.
Mappages de LUN	Vérifiez que les LUN sont mappées sur un groupe initiateur. Sur la console du système de stockage, vous pouvez utiliser l'une des commandes suivantes : • `lun mapping show` Affiche toutes les LUN et les groupes initiateurs sur lesquels ils sont mappés. • `lun mapping show -igroup` Affiche les LUN mappées sur un groupe initiateur spécifique.

Paramètre de configuration	Que faire
Activation des LIF iSCSI	Vérifiez que les interfaces logiques iSCSI sont activées.

Informations associées

- "Matrice d'interopérabilité NetApp"
- "les mappages de lun s'affichent"

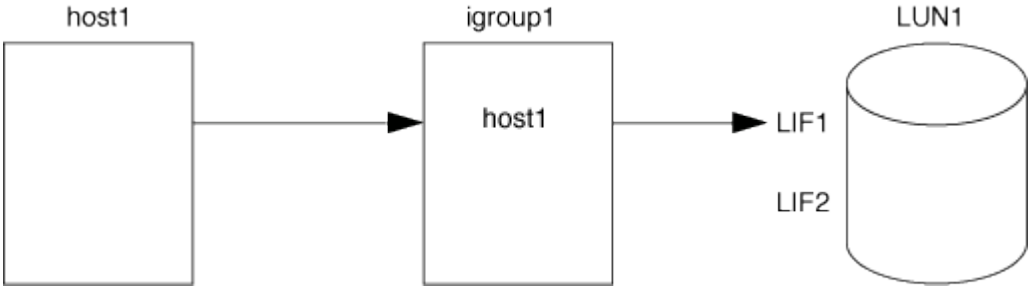
Gestion des igroups et des ensembles de ports

Moyens de limiter l'accès aux LUN avec des ensembles de ports et des igroups

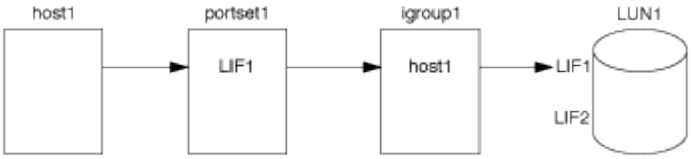
En plus d'utiliser le mappage de LUN sélectif (SLM), vous pouvez limiter l'accès à vos LUN via des igroups et des ensembles de ports.

Les ensembles de ports peuvent être utilisés avec SLM pour restreindre davantage l'accès de certaines cibles à certains initiateurs. Lors de l'utilisation de SLM avec des ensembles de ports, les LUN sont accessibles sur l'ensemble des LIF du portset sur le nœud propriétaire de la LUN et sur le partenaire HA de ce nœud.

Dans l'exemple suivant, initiator1 n'a pas de jeu de ports. Sans ensemble de ports, initiator1 peut accéder à LUN1 via LIF1 et LIF2.



Vous pouvez limiter l'accès à LUN1 en utilisant un ensemble de ports. Dans l'exemple suivant, initiator1 ne peut accéder à LUN1 que via LIF1. Cependant, initiator1 ne peut pas accéder à LUN1 via LIF2 car LIF2 n'est pas dans portset1.



Informations associées

- Mappage de LUN sélectif
- Créer un ensemble de ports et lier à un groupe initiateur

Affichez et gérez les initiateurs SAN et igroups

Vous pouvez utiliser System Manager pour afficher et gérer les groupes initiateurs et les initiateurs.

Description de la tâche

- Les groupes initiateurs identifient les hôtes pouvant accéder à des LUN spécifiques sur le système de stockage.
- Une fois qu'un initiateur et des groupes initiateurs sont créés, vous pouvez également les modifier ou les supprimer.
- Pour gérer les groupes initiateurs SAN et les initiateurs, vous pouvez effectuer les tâches suivantes :
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

Afficher et gérer les groupes initiateurs SAN

Vous pouvez utiliser System Manager pour afficher la liste des groupes initiateurs. Dans cette liste, vous pouvez effectuer des opérations supplémentaires.

Étapes

1. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

   La page affiche la liste des groupes initiateurs. Si la liste est grande, vous pouvez afficher des pages supplémentaires de la liste en cliquant sur les numéros de page dans le coin inférieur droit de la page.

   Les colonnes affichent diverses informations sur les igroups. Depuis 9.11.1, l'état de connexion du groupe initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.

2. (Facultatif) : vous pouvez effectuer les tâches suivantes en cliquant sur les icônes dans le coin supérieur droit de la liste :
   - **Recherche**
   - **Télécharger** la liste.
   - **Afficher** ou **Masquer** dans la liste.
   - **Filtrer** les données de la liste.
3. Vous pouvez effectuer des opérations à partir de la liste :
   - Cliquez sur + Add pour ajouter un groupe initiateur.
   - Cliquez sur le nom du groupe initiateur pour afficher la page **Présentation** qui affiche les détails sur le groupe initiateur.

     Sur la page **Présentation**, vous pouvez afficher les LUN associées au groupe initiateur et lancer les opérations pour créer des LUN et mapper les LUN. Cliquez sur **tous les initiateurs SAN** pour revenir à la liste principale.

   - Passez la souris sur le groupe initiateur, puis cliquez sur ⋮ en regard de son nom pour modifier ou supprimer ce groupe.
   - Passez le curseur de la souris sur la zone à gauche du nom du groupe initiateur, puis cochez la case. Si vous cliquez sur **+Ajouter au groupe initiateur**, vous pouvez ajouter ce groupe initiateur à un autre groupe initiateur.
   - Dans la colonne **Storage VM**, cliquez sur le nom d'une machine virtuelle de stockage pour en afficher les détails.

Afficher et gérer les initiateurs SAN

Vous pouvez utiliser System Manager pour afficher la liste des initiateurs. Dans cette liste, vous pouvez effectuer des opérations supplémentaires.

Étapes

1. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

   La page affiche la liste des groupes initiateurs.

2. Pour afficher les initiateurs, effectuez les opérations suivantes :

   - Cliquez sur l'onglet **FC Initiators** pour afficher la liste des initiateurs FC.
   - Cliquez sur l'onglet **initiateurs iSCSI** pour afficher la liste des initiateurs iSCSI.

     Les colonnes affichent diverses informations relatives aux initiateurs.

   Depuis 9.11.1, le statut de connexion de l'initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.

3. (Facultatif) : vous pouvez effectuer les tâches suivantes en cliquant sur les icônes dans le coin supérieur droit de la liste :
   - **Rechercher** la liste des initiateurs particuliers.
   - **Télécharger** la liste.
   - **Afficher** ou **Masquer** dans la liste.
   - **Filtrer** les données de la liste.

Créez un groupe initiateur imbriqué

À partir de la version ONTAP 9.9.1, vous pouvez créer un groupe initiateur qui se compose d'autres groupes initiateurs existants.

1. Dans System Manager, cliquez sur **hôte > groupes d'initiateurs SAN**, puis sur **Ajouter**.
2. Saisissez le nom **Nom** et **Description** du groupe initiateur.

   La description sert d'alias de groupe initiateur.

3. Sélectionnez **Storage VM** et **Host Operating System**.

   > Impossible de modifier le type de système d'exploitation d'un groupe initiateur imbriqué après la création du groupe initiateur.

4. Sous **membres du groupe initiateur**, sélectionnez **Groupe initiateur existant**.

   Vous pouvez utiliser **Search** pour rechercher et sélectionner les groupes d'initiateurs à ajouter.

Mappez les igroups sur plusieurs LUN

Depuis la version ONTAP 9.9.1, vous pouvez mapper les groupes initiateurs sur deux ou plusieurs LUN simultanément.

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Sélectionnez les LUN à mapper.
3. Cliquez sur **plus**, puis sur **mapper aux groupes initiateurs**.

> Les igroups sélectionnés sont ajoutés aux LUN sélectionnés. Les mappages existants ne sont pas écrasés.

Créer un ensemble de ports et lier à un groupe initiateur

En plus de l'utilisation "Mappage de LUN sélectif (SLM)", Vous pouvez créer un ensemble de ports et lier l'ensemble de ports à un groupe initiateur pour limiter davantage les LIF qu'un initiateur peut utiliser pour accéder à une LUN.

Si vous n'associez pas un ensemble de ports à un groupe initiateur, tous les initiateurs du groupe initiateur peuvent accéder aux LUN mappées par l'intermédiaire de toutes les LIF du nœud propriétaire de la LUN et du partenaire haute disponibilité du nœud propriétaire.

Avant de commencer

Vous devez disposer d'au moins une LIF et un groupe initiateur.

Sauf si vous utilisez des groupes d'interface, deux LIF sont recommandées pour la redondance des protocoles iSCSI et FC. Une seule LIF est recommandée pour les groupes d'interfaces.

Description de la tâche

Il est avantageux d'utiliser des ensembles de ports avec SLM lorsque vous disposez de plus de deux LIF sur un nœud et que vous souhaitez limiter un certain initiateur à un sous-ensemble de LIF. Sans portsets, toutes les cibles du nœud sont accessibles par tous les initiateurs avec accès à la LUN via le nœud propriétaire de la LUN et le partenaire haute disponibilité du nœud propriétaire.

Exemple 6. Étapes

System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour créer des ensembles de ports et les lier aux groupes initiateurs.

Si vous devez créer un ensemble de ports et le lier à un groupe initiateur dans une version de ONTAP antérieure à 9.10.1, vous devez utiliser la procédure de l'interface de ligne de commandes de ONTAP.

À partir d'ONTAP 9.12.1, si vous ne disposez pas d'un ensemble de ports existant, vous devez créer le premier à l'aide de la procédure ONTAP CLI.

1. Dans System Manager, cliquez sur **réseau > Présentation > ensembles de ports**, puis sur **Ajouter**.
2. Entrez les informations du nouvel ensemble de ports et cliquez sur **Ajouter**.
3. Cliquez sur **hôtes > SAN Initiator Groups**.
4. Pour lier l'ensemble de ports à un nouveau groupe initiateur, cliquez sur **Ajouter**.

   Pour lier le génération à un groupe initiateur existant, sélectionnez-le, cliquez sur ⋮, puis sur **Modifier le groupe initiateur**.

Informations associées

"Afficher et gérer les initiateurs et les igroups"

CLI

1. Créer un jeu de ports contenant les LIFs appropriées :

   ```
   portset create -vserver vserver_name -portset portset_name -protocol
   protocol -port-name port_name
   ```

   Si vous utilisez FC, spécifiez le `protocol` ens. paramètre `fcp`. Si vous utilisez iSCSI, spécifiez `protocol` ens. paramètre `iscsi`.

2. Connectez le groupe initiateur à l'ensemble de ports :

   ```
   lun igroup bind -vserver vserver_name -igroup igroup_name -portset
   portset_name
   ```

   Pour en savoir plus, `lun igroup bind` consultez le "Référence de commande ONTAP".

3. Vérifiez que vos jeux de ports et vos LIF sont corrects :

   ```
   portset show -vserver vserver_name
   ```

   ```
   Vserver   Portset   Protocol Port Names    Igroups
   --------- --------- -------- ------------- --------
   vs3       portset0  iscsi    lif0,lif1     igroup1
   ```

Gérer les ensembles de ports

En plus de "Mappage de LUN sélectif (SLM)", Vous pouvez utiliser des ensembles de ports pour limiter davantage les LIF qu'un initiateur peut utiliser pour accéder à une LUN.

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les interfaces réseau associées aux ensembles de ports et supprimer les ensembles de ports.

Modifier les interfaces réseau associées à un ensemble de ports

1. Dans System Manager, sélectionnez **réseau > Présentation > Portsets**.
2. Sélectionnez la génération que vous souhaitez modifier, puis ⋮ sélectionnez **Modifier génération**.

Supprimer un ensemble de ports

1. Dans System Manager, cliquez sur **réseau > Présentation > ensembles de ports**.
2. Pour supprimer un seul ensemble de ports, sélectionnez-le, ⋮ puis sélectionnez **Supprimer les ensembles de ports**.

   Pour supprimer plusieurs ensembles de ports, sélectionnez-les et cliquez sur **Supprimer**.

Présentation du mappage de LUN sélectif

Le mappage de LUN sélectif (SLM) réduit le nombre de chemins entre l'hôte et la LUN. Avec SLM, lorsqu'un nouveau mappage de LUN est créé, le LUN est accessible uniquement via des chemins sur le nœud propriétaire de la LUN et son partenaire HA.

SLM permet de gérer un groupe initiateur unique par hôte et prend également en charge les opérations de déplacement de LUN sans interruption qui ne nécessitent pas de manipulation de l'ensemble de ports ou de remappage des LUN.

"Ensembles de ports" Peut être utilisé avec SLM pour restreindre davantage l'accès à certaines cibles à certains initiateurs. Lors de l'utilisation de SLM avec des ensembles de ports, les LUN sont accessibles sur l'ensemble des LIF du portset sur le nœud propriétaire de la LUN et sur le partenaire HA de ce nœud.

SLM est activé par défaut sur tous les nouveaux mappages de LUN.

Déterminez si SLM est activé sur un mappage de LUN

Si votre environnement comporte une combinaison de LUN créées dans une version de ONTAP 9 et de LUN faisant l'objet d'une transition à partir de versions précédentes, vous devrez peut-être déterminer si la fonction de mappage de LUN sélectif (SLM) est activée sur une LUN spécifique.

Vous pouvez utiliser les informations affichées dans la sortie du `lun mapping show -fields reporting-nodes, node` Commande permettant de déterminer si SLM est activé sur votre mappage de LUN. Si SLM n'est pas activé, "-" s'affiche dans les cellules sous la colonne "nœuds de portage" de la sortie de la commande. Si SLM est activé, la liste des nœuds affichée sous la colonne « noeuds » est dupliquée dans la colonne « noeuds de portage ».

Pour en savoir plus, `lun mapping show` consultez le "Référence de commande ONTAP".

Modifiez la liste des noeuds-rapports SLM

Si vous déplacez une LUN ou un volume contenant des LUN vers une autre paire haute disponibilité (HA) au sein du même cluster, vous devez modifier la liste des nœuds de rapport du mappage de LUN sélectif (SLM) avant de lancer le déplacement pour vous assurer que les chemins LUN actifs et optimisés sont maintenus.

Étapes

1. Ajoutez le nœud de destination et son nœud partenaire à la liste « reporting-nodes » de l'agrégat ou du volume :

   ```
   lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
   -igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
   destination-volume <volume_name>]
   ```

   Si vous disposez d'une nomenclature établie cohérente, vous pouvez modifier plusieurs mappages de LUN en même temps en utilisant à `igroup_prefix*` la place de `igroup_name`.

2. Relancez l'analyse de l'hôte pour détecter les nouveaux chemins ajoutés.
3. Si votre système d'exploitation le requiert, ajoutez les nouveaux chemins d'accès à votre configuration MPIO (Multi-Path Network I/O).
4. Exécutez la commande pour l'opération de déplacement requise et attendez la fin de l'opération.
5. Vérifier que les E/S sont en cours de maintenance via le chemin actif/optimisé :

   ```
   lun mapping show -fields reporting-nodes
   ```

6. Supprimez l'ancien propriétaire de LUN et son nœud partenaire de la liste noeuds-rapports :

   ```
   lun mapping remove-reporting-nodes -vserver <vserver_name> -path
   <lun_path> -igroup <igroup_name> -remote-nodes
   ```

7. Vérifiez que la LUN a été supprimée du mappage de LUN existant :

   ```
   lun mapping show -fields reporting-nodes
   ```

8. Supprimez toute entrée de périphérique obsolète pour le système d'exploitation hôte.
9. Modifiez les fichiers de configuration des chemins d'accès multiples si nécessaire.
10. Relancez l'analyse de l'hôte pour vérifier la suppression des anciens chemins.
    Reportez-vous à la documentation de votre hôte pour connaître les étapes spécifiques à suivre pour relancer l'analyse de vos hôtes.

Gérez le protocole iSCSI

Configurez votre réseau pour des performances optimales

Les performances des réseaux Ethernet varient considérablement. Vous pouvez optimiser les performances du réseau utilisé pour iSCSI en sélectionnant des valeurs de configuration spécifiques.

Étapes

1. Connectez l'hôte et les ports de stockage au même réseau.

   Il est préférable de se connecter aux mêmes commutateurs. Le routage ne doit jamais être utilisé.

2. Sélectionnez les ports à vitesse la plus élevée disponibles et dédier-les à iSCSI.

   Les 10 ports GbE sont optimaux. Le nombre minimal de ports 1 GbE est égal à 1.

3. Désactiver le contrôle de flux Ethernet pour tous les ports.

   Vous devriez voir "Gestion du réseau" Pour configurer le contrôle de flux du port Ethernet à l'aide de l'interface de ligne de commande.

4. Activez les trames Jumbo (généralement MTU de 9 9000).

   Tous les périphériques du chemin d'accès aux données, y compris les initiateurs, les cibles et les commutateurs, doivent prendre en charge les trames Jumbo. Dans le cas contraire, l'activation des trames Jumbo réduit considérablement les performances du réseau.

Configuration d'un SVM pour iSCSI

Pour configurer un SVM (Storage Virtual machine) pour iSCSI, vous devez créer des LIFs pour le SVM et affecter le protocole iSCSI à ces LIFs.

Description de la tâche

Au moins une LIF iSCSI par nœud est nécessaire pour chaque SVM assurant le service des données avec le protocole iSCSI. Pour la redondance, vous devez créer au moins deux LIF par nœud.

Exemple 7. Étapes

System Manager

Configurer une machine virtuelle de stockage pour iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer iSCSI sur une nouvelle machine virtuelle de stockage	Pour configurer iSCSI sur une machine virtuelle de stockage existante
1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**. 2. Entrez un nom pour la machine virtuelle de stockage. 3. Sélectionnez **iSCSI** pour le **Protocole d'accès**. 4. Cliquez sur **Activer iSCSI** et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + chaque nœud doit disposer d'au moins deux interfaces réseau. 5. Cliquez sur **Enregistrer**.	1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**. 2. Cliquez sur la VM de stockage que vous souhaitez configurer. 3. Cliquez sur l'onglet **Paramètres**, puis cliquez sur ⚙ en regard du protocole iSCSI. 4. Cliquez sur **Activer iSCSI** et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + chaque nœud doit disposer d'au moins deux interfaces réseau. 5. Cliquez sur **Enregistrer**.

CLI

Configurer une VM de stockage pour iSCSI à l'aide de l'interface de ligne de commande ONTAP.

1. Activer les SVM pour écouter le trafic iSCSI :

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. Créer une LIF pour les SVM sur chaque nœud à utiliser pour iSCSI :
   - Pour ONTAP 9.6 et versions ultérieures :

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - Pour ONTAP 9.5 et versions antérieures :

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. Vérifiez que vous avez configuré correctement vos LIF :

   ```
   network interface show -vserver vserver_name
   ```

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

4. Vérifier que iSCSI est actif et que l'IQN cible pour ce SVM :

```
vserver iscsi show -vserver vserver_name
```

5. Depuis votre hôte, créez des sessions iSCSI vers vos LIF.

Informations associées

- "Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"

Définir une méthode de stratégie de sécurité pour un initiateur

Vous pouvez définir une liste d'initiateurs et leurs méthodes d'authentification. Vous pouvez également modifier la méthode d'authentification par défaut qui s'applique aux initiateurs qui n'ont pas de méthode d'authentification définie par l'utilisateur.

Description de la tâche

Vous pouvez générer des mots de passe uniques à l'aide d'algorithmes de règles de sécurité dans le produit ou vous pouvez spécifier manuellement les mots de passe que vous souhaitez utiliser.

> Tous les initiateurs ne prennent pas en charge les mots de passe secrets CHAP hexadécimaux.

Étapes

1. Utilisez le `vserver iscsi security create` commande permettant de créer une méthode de stratégie de sécurité pour un initiateur.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
   ```

2. Suivez les commandes à l'écran pour ajouter les mots de passe.

   Crée une méthode de stratégie de sécurité pour l'initiateur iqn.1991-05.com.microsoft:host1 avec des noms d'utilisateur et des mots de passe CHAP entrants et sortants.

Informations associées

- Fonctionnement de l'authentification iSCSI
- Authentification CHAP

Suppression d'un service iSCSI pour une SVM

Vous pouvez supprimer un service iSCSI pour une machine virtuelle de stockage (SVM) s'il n'est plus nécessaire.

Avant de commencer

L'état d'administration du service iSCSI doit être à l'état "down" avant de pouvoir supprimer un service iSCSI. Vous pouvez déplacer l'état d'administration vers le bas à l'aide de `vserver iscsi modify` commande.

Étapes

1. Utilisez le `vserver iscsi modify` Commande permettant d'arrêter les E/S vers la LUN.

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. Utilisez le `vserver iscsi delete` Commande permettant de supprimer le service iscsi du SVM.

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. Utilisez le `vserver iscsi show command` Pour vérifier que vous avez supprimé le service iSCSI de la SVM.

   ```
   vserver iscsi show -vserver vs1
   ```

Obtenez plus de détails dans les restaurations d'erreurs de session iSCSI

L'augmentation du niveau de récupération des erreurs de session iSCSI vous permet de recevoir des informations plus détaillées sur les restaurations d'erreurs iSCSI. L'utilisation d'un niveau de récupération d'erreur plus élevé peut entraîner une réduction mineure des performances de la session iSCSI.

Description de la tâche

Par défaut, ONTAP est configuré pour utiliser le niveau de récupération d'erreur 0 pour les sessions iSCSI. Si vous utilisez un initiateur qui a été qualifié pour la récupération d'erreur de niveau 1 ou 2, vous pouvez choisir d'augmenter le niveau de récupération d'erreur. Le niveau de récupération d'erreur de session modifié n'affecte que les sessions nouvellement créées et n'affecte pas les sessions existantes.

À partir de ONTAP 9.4, le `max-error-recovery-level` cette option n'est pas prise en charge dans le `iscsi show` et `iscsi modify` commandes.

Étapes

1. Entrer en mode avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez le paramètre actuel à l'aide du `iscsi show` commande.

   ```
   iscsi show -vserver vs3 -fields max-error-recovery-level
   ```

   ```
   vserver max-error-recovery-level
   ------- ------------------------
   vs3     0
   ```

3. Modifiez le niveau de récupération d'erreur à l'aide de `iscsi modify` commande.

   ```
   iscsi modify -vserver vs3 -max-error-recovery-level 2
   ```

Enregistrez le SVM avec un serveur iSNS

Vous pouvez utiliser le `vserver iscsi isns` Commande permettant de configurer la machine virtuelle de stockage (SVM) à enregistrer avec un serveur iSNS.

Description de la tâche

Le `vserver iscsi isns create` Commande permet de configurer le SVM pour qu'il s'enregistre avec le serveur iSNS. Le SVM ne fournit pas de commandes permettant de configurer ou de gérer le serveur iSNS. Pour gérer le serveur iSNS, vous pouvez utiliser les outils d'administration du serveur ou l'interface fournie par le fournisseur pour le serveur iSNS.

Étapes

1. Sur votre serveur iSNS, assurez-vous que votre service iSNS est opérationnel et disponible.
2. Créer la LIF de SVM management sur un port data :

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

   Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

3. Créer un service iSCSI sur votre SVM si celui-ci n'existe pas déjà :

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Vérifiez que le service iSCSI a été créé avec succès :

   ```
   iscsi show -vserver SVM_name
   ```

5. Vérifier qu'une route par défaut existe pour le SVM :

   ```
   network route show -vserver SVM_name
   ```

6. Si une route par défaut n'existe pas pour le SVM, créer une route par défaut :

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

   Pour en savoir plus, `network route create` consultez le "Référence de commande ONTAP".

7. Configurer le SVM pour s'enregistrer avec le service iSNS :

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   Les familles d'adresses IPv4 et IPv6 sont prises en charge. La famille d'adresses du serveur iSNS doit être identique à celle du LIF de gestion des SVM.

   Par exemple, vous ne pouvez pas connecter une LIF de gestion SVM avec une adresse IPv4 à un serveur iSNS avec une adresse IPv6.

8. Vérifiez que le service iSNS fonctionne :

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. Si le service iSNS n'est pas en cours d'exécution, démarrez-le :

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

Résolution des messages d'erreur iSCSI sur le système de stockage

Vous pouvez afficher un certain nombre de messages d'erreur iSCSI courants avec le `event log show` commande. Vous devez savoir ce que signifient ces messages et ce que vous pouvez faire pour résoudre les problèmes qu'ils identifient.

Le tableau suivant contient les messages d'erreur les plus courants et des instructions pour les résoudre :

Messagerie	Explication	Que faire
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	Le service iSCSI n'est pas activé sur l'interface.	Vous pouvez utiliser le `iscsi interface enable` Pour activer le service iSCSI sur l'interface. Par exemple : `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	CHAP n'est pas configuré correctement pour l'initiateur spécifié.	Vous devez vérifier les paramètres CHAP ; vous ne pouvez pas utiliser le même nom d'utilisateur et mot de passe pour les paramètres entrant et sortant sur le système de stockage : • Les identifiants entrants du système de stockage doivent correspondre aux informations d'identification sortantes de l'initiateur. • Les identifiants sortants du système de stockage doivent correspondre aux informations d'identification entrantes de l'initiateur.

Pour en savoir plus, `event log show` consultez le "Référence de commande ONTAP".

Activer ou désactiver le basculement automatique de LIF iSCSI

Après la mise à niveau vers ONTAP 9.11.1 ou une version ultérieure, vous devez activer manuellement le basculement automatique des LIF sur toutes les LIF iSCSI créées dans ONTAP 9.10.1 ou une version antérieure.

À partir de la version ONTAP 9.11.1, vous pouvez activer le basculement automatique des LIF iSCSI sur les plateformes SAN 100 % Flash. En cas de basculement du stockage, la LIF iSCSI est automatiquement migrée de son nœud ou port de rattachement vers son nœud ou port partenaire haute disponibilité, puis de nouveau une fois le basculement terminé. Ou, si le port de la LIF iSCSI devient défectueux, la LIF est automatiquement migrée vers un port sain de son nœud de rattachement actuel, puis de nouveau vers son port d'origine une fois le port refonctionnel. Permet aux charges de travail SAN exécutées sur iSCSI de reprendre plus rapidement le service d'E/S après un basculement.

Dans ONTAP 9.11.1 et versions ultérieures, par défaut, les LIF iSCSI nouvellement créées sont activées pour le basculement automatique des LIF, si l'une des conditions suivantes est vraie :

- Il n'y a pas de LIF iSCSI sur le SVM
- Toutes les LIFs iSCSI sur le SVM sont activées pour le basculement automatique des LIF

Activer le basculement automatique de LIF iSCSI

Par défaut, les LIF iSCSI créées dans ONTAP 9.10.1 et les versions antérieures ne sont pas activées pour le basculement automatique des LIF. Si sur le SVM des LIF iSCSI ne sont pas activées pour le basculement automatique des LIF, vos nouvelles LIF ne seront pas non plus activées pour le basculement automatique des LIF. Si le basculement automatique de LIF n'est pas activé et qu'un événement de basculement se produit, vos LIFs iSCSI ne migrent pas.

En savoir plus sur "Basculement et rétablissement de LIF".

Étape

1. Activer le basculement automatique pour une LIF iSCSI :

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

   Pour mettre à jour toutes les LIFs iSCSI sur le SVM, utiliser `-lif*` au lieu de `lif`.

Désactivez le basculement automatique des LIF iSCSI

Si vous avez précédemment activé le basculement automatique de LIF iSCSI sur des LIF iSCSI créées dans ONTAP 9.10.1 ou une version antérieure, vous avez la possibilité de le désactiver.

Étape

1. Désactiver le basculement automatique pour une LIF iSCSI :

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

   Pour mettre à jour toutes les LIFs iSCSI sur le SVM, utiliser `-lif*` au lieu de `lif`.

Informations associées

- "Créer une LIF"
- Manuellement "Migrer une LIF"
- Manuellement "Restaure une LIF sur son port d'attache"
- "Configurer les paramètres de basculement sur une LIF"

Gestion du protocole FC

Configuration d’un SVM pour FC

Pour configurer un SVM (Storage Virtual machine) pour FC, vous devez créer des LIFs pour le SVM et affecter le protocole FC à ces LIFs.

Avant de commencer

Vous devez disposer d’une licence FC ("Inclus avec ONTAP One") et l’activer. Si la licence FC n’est pas activée, les LIFs et les SVM semblent être en ligne mais le statut opérationnel sera `down`. Le service FC doit être activé pour que vos LIF et SVM soient opérationnels. Vous devez utiliser un zoning unique pour toutes les LIFs FC du SVM pour héberger les initiateurs.

Description de la tâche

NetApp prend en charge au moins une LIF FC par nœud pour chaque SVM assurant le service des données avec le protocole FC. Vous devez utiliser deux LIF par nœud et deux structures, avec une LIF par nœud attaché. Cela permet la redondance au niveau de la couche des nœuds et de la structure.

Exemple 8. Étapes

System Manager

Configurer une machine virtuelle de stockage pour iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer FC sur une nouvelle machine virtuelle de stockage	Pour configurer FC sur une machine virtuelle de stockage existante
1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**. 2. Entrez un nom pour la machine virtuelle de stockage. 3. Sélectionnez **FC** pour **Protocole d'accès**. 4. Cliquez sur **Activer FC**. + les ports FC sont attribués automatiquement. 5. Cliquez sur **Enregistrer**.	1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**. 2. Cliquez sur la VM de stockage que vous souhaitez configurer. 3. Cliquez sur l'onglet **Settings**, puis cliquez sur ⚙ en regard du protocole FC. 4. Cliquez sur **Activer FC** et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + les ports FC sont attribués automatiquement. 5. Cliquez sur **Enregistrer**.

CLI

1. Activer le service FC sur le SVM :

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. Créez deux LIF pour les SVM sur chaque nœud assurant le service FC :
   - Pour ONTAP 9.6 et versions ultérieures :

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - Pour ONTAP 9.5 et versions antérieures :

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Vérifiez que vos LIF ont été créées et que leur statut opérationnel est `online`:

   ```
   network interface show -vserver vserver_name lif_name
   ```

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

Informations associées

- "Support NetApp"
- "Matrice d'interopérabilité NetApp"

- Considérations relatives aux LIF dans les environnements cluster SAN

Suppression d'un service FC pour une SVM

Vous pouvez supprimer un service FC pour une machine virtuelle de stockage (SVM) s'il n'est plus nécessaire.

Avant de commencer

Le statut d'administration doit être « down » avant de supprimer un service FC pour une SVM. Vous pouvez définir l'état d'administration sur Down avec l'un ou l'autre `vserver fcp modify` commande ou le `vserver fcp stop` commande.

Étapes

1. Utilisez le `vserver fcp stop` Commande permettant d'arrêter les E/S vers la LUN.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. Utilisez le `vserver fcp delete` Commande permettant de supprimer le service du SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. Utilisez le `vserver fcp show` Pour vérifier que vous avez supprimé le service FC de votre SVM :

   ```
   vserver fcp show -vserver vs_1
   ```

Configurations MTU recommandées pour les trames jumbo FCoE

Pour la technologie Fibre Channel over Ethernet (FCoE), les trames jumbo pour la partie adaptateur Ethernet de la carte CNA doivent être configurées à 9000 MTU. Les trames Jumbo pour la partie adaptateur FCoE du CNA doivent être configurées à plus de 10 1500 MTU. Ne configurez les trames Jumbo que si l'initiateur, la cible et tous les commutateurs d'intervention prennent en charge et sont configurés pour les trames Jumbo.

Gérez le protocole NVMe

Démarrer le service NVMe pour un SVM

Avant de pouvoir utiliser le protocole NVMe sur votre SVM, vous devez démarrer le service NVMe sur la SVM.

Avant de commencer

NVMe doit être autorisé en tant que protocole sur votre système.

Les protocoles NVMe suivants sont pris en charge :

Protocole	À partir de …	Autorisé par…
TCP	ONTAP 9.10.1	Valeur par défaut

FCP	ONTAP 9.4	Valeur par défaut

Étapes

1. Modifiez le paramètre de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez que NVMe est autorisé en tant que protocole :

   ```
   vserver nvme show
   ```

3. Créez le service de protocole NVMe :

   ```
   vserver nvme create
   ```

4. Démarrer le service de protocole NVMe sur le SVM :

   ```
   vserver nvme modify -status -admin up
   ```

Suppression du service NVMe d'un SVM

Si nécessaire, vous pouvez supprimer le service NVMe de votre SVM (Storage Virtual machine).

Étapes

1. Modifiez le paramètre de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Arrêter le service NVMe sur le SVM :

   ```
   vserver nvme modify -status -admin down
   ```

3. Supprimez le service NVMe :

   ```
   vserver nvme delete
   ```

Redimensionner un espace de noms

Depuis la version ONTAP 9.10.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour augmenter ou réduire la taille d'un espace de noms NVMe. System Manager peut être utilisé pour augmenter la taille d'un namespace NVMe.

Augmenter la taille d'un namespace

System Manager

1. Cliquez sur **stockage > espaces de noms NVMe**.
2. Hoover sur l'espace de noms que vous voulez augmenter, cliquez sur ⋮, puis cliquez sur **Modifier**.
3. Sous **CAPACITY**, modifiez la taille de l'espace de noms.

CLI

1. Saisissez la commande suivante : `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `–size` *`new_size_of_namespace`*

Réduire la taille d'un namespace

Vous devez utiliser l'interface de ligne de commandes de ONTAP pour réduire la taille d'un namespace NVMe.

1. Modifiez le paramètre de privilège sur avancé :

   ```
   set –privilege advanced
   ```

2. Diminuer la taille du namespace :

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

Convertir un namespace en LUN

Depuis la version ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour convertir un espace de noms NVMe existant en LUN sans déplacement.

Avant de commencer

- L'espace de noms NVMe spécifié ne doit pas disposer d'aucun mappage existant à un sous-système.
- L'espace de noms ne doit pas faire partie d'un snapshot ou du côté destination de la relation SnapMirror comme un espace de noms en lecture seule.
- Les espaces de noms NVMe ne sont pris en charge qu'avec des plates-formes spécifiques et des cartes réseau, cette fonctionnalité ne fonctionne qu'avec du matériel spécifique.

Étapes

1. Entrez la commande suivante pour convertir un namespace NVMe en LUN :

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

   Pour en savoir plus, `lun convert-from-namespace` consultez le "Référence de commande ONTAP".

Configuration de l'authentification intrabande sur NVMe

Depuis ONTAP 9.12.1, vous pouvez utiliser l'interface de ligne de commande ONTAP pour configurer l'authentification intrabande (sécurisée), bidirectionnelle et unidirectionnelle entre un hôte et un contrôleur NVMe via les protocoles NVME/TCP et

NVMe/FC à l’aide de l’authentification DH-HMAC-CHAP. À partir de ONTAP 9.14.1, l’authentification intrabande peut être configurée dans System Manager.

Pour configurer l’authentification intrabande, chaque hôte ou contrôleur doit être associé à une clé DH-HMAC-CHAP qui est une combinaison du NQN de l’hôte ou du contrôleur NVMe et d’un secret d’authentification configuré par l’administrateur. Pour qu’un hôte ou un contrôleur NVMe authentifie son homologue, il doit connaître la clé associée à celui-ci.

Dans l’authentification unidirectionnelle, une clé secrète est configurée pour l’hôte, mais pas pour le contrôleur. Dans le cas d’une authentification bidirectionnelle, une clé secrète est configurée pour l’hôte et le contrôleur.

SHA-256 est la fonction de hachage par défaut et 2048 bits est le groupe DH par défaut.

System Manager

Depuis ONTAP 9.14.1, vous pouvez utiliser System Manager pour configurer l'authentification intrabande lors de la création ou de la mise à jour d'un sous-système NVMe, de la création ou du clonage d'espaces de noms NVMe, ou de l'ajout de groupes de cohérence avec de nouveaux espaces de noms NVMe.

Étapes

1. Dans System Manager, cliquez sur **hosts > NVMe Subsystem**, puis sur **Add**.
2. Ajoutez le nom du sous-système NVMe, puis sélectionnez la VM de stockage et le système d'exploitation hôte.
3. Saisissez le NQN hôte.
4. Sélectionnez **utiliser l'authentification intrabande** en regard du NQN hôte.
5. Indiquez le secret de l'hôte et le secret du contrôleur.

   La clé DH-HMAC-CHAP est une combinaison du NQN de l'hôte ou du contrôleur NVMe et d'un secret d'authentification configuré par l'administrateur.

6. Sélectionnez la fonction de hachage et le groupe DH de votre choix pour chaque hôte.

   Si vous ne sélectionnez pas de fonction de hachage et de groupe DH, SHA-256 est affecté comme fonction de hachage par défaut et 2048 bits comme groupe DH par défaut.

7. Si vous le souhaitez, cliquez sur **Ajouter** et répétez les étapes nécessaires pour ajouter d'autres hôtes.
8. Cliquez sur **Enregistrer**.
9. Pour vérifier que l'authentification intrabande est activée, cliquez sur **System Manager > hosts > NVMe Subsystem > Grid > Peek View**.

   Une icône de clé transparente en regard du nom d'hôte indique que le mode unidirectionnel est activé. Une clé opaque en regard du nom d'hôte indique que le mode bidirectionnel est activé.

CLI

Étapes

1. Ajoutez l'authentification DH-HMAC-CHAP à votre sous-système NVMe :

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   Pour en savoir plus, `vserver nvme subsystem host add` consultez le "Référence de commande ONTAP".

2. Vérifiez que le protocole d'authentification CHAP DH-HMAC est ajouté à votre hôte :

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Pour en savoir plus, `vserver nvme subsystem host show` consultez le "Référence de commande ONTAP".

3. Vérifier que l'authentification DH-HMAC CHAP a été effectuée lors de la création du contrôleur NVMe :

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Pour en savoir plus, `vserver nvme subsystem controller show` consultez le "Référence de commande ONTAP".

Désactivez l'authentification intrabande sur NVMe

Si vous avez configuré l'authentification intrabande sur NVMe à l'aide de DH-HMAC-CHAP, vous pouvez choisir de la désactiver à tout moment.

Si vous revenez de ONTAP 9.12.1 ou version ultérieure à ONTAP 9.12.0 ou version antérieure, vous devez désactiver l'authentification intrabande avant de revenir à cette version. Si l'authentification intrabande à l'aide de DH-HMAC-CHAP n'est pas désactivée, le retour échoue.

Étapes

1. Supprimez l'hôte du sous-système pour désactiver l'authentification DH-HMAC-CHAP :

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Vérifiez que le protocole d'authentification DH-HMAC-CHAP est supprimé de l'hôte :

```
vserver nvme subsystem host show
```

3. Ajoutez l'hôte au sous-système sans authentification :

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Configuration du canal sécurisé TLS pour NVMe/TCP

À partir de ONTAP 9.16.1, vous pouvez configurer le canal sécurisé TLS pour les connexions NVMe/TCP. Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour ajouter un nouveau sous-système NVMe avec TLS activé ou activer TLS pour un sous-système NVMe existant.

System Manager

Depuis la version ONTAP 9.16.1, vous pouvez utiliser System Manager pour configurer TLS pour les connexions NVMe/TCP lors de la création ou de la mise à jour d'un sous-système NVMe, de la création ou du clonage d'espaces de noms NVMe, ou de l'ajout de groupes de cohérence avec de nouveaux espaces de noms NVMe.

Étapes

1. Dans System Manager, cliquez sur **hosts > NVMe Subsystem**, puis sur **Add**.
2. Ajoutez le nom du sous-système NVMe, puis sélectionnez la VM de stockage et le système d'exploitation hôte.
3. Saisissez le NQN hôte.
4. Sélectionnez **exiger le protocole TLS (transport Layer Security)** en regard du NQN hôte.
5. Fournissez la clé pré-partagée (PSK).
6. Cliquez sur **Enregistrer**.
7. Pour vérifier que le canal sécurisé TLS est activé, sélectionnez **System Manager > hosts > NVMe Subsystem > Grid > Peek View**.

CLI

Étapes

1. Ajoutez un hôte de sous-système NVMe qui prend en charge le canal sécurisé TLS. Vous pouvez fournir une clé pré-partagée (PSK) en utilisant le `tls-configured-psk` argument:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Vérifiez que l'hôte du sous-système NVMe est configuré pour le canal sécurisé TLS. Vous pouvez éventuellement utiliser l' `tls-key-type`argument pour afficher uniquement les hôtes qui utilisent ce type de clé :

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Vérifiez que le contrôleur hôte du sous-système NVMe est configuré pour le canal sécurisé TLS. Vous pouvez éventuellement utiliser l'un des `tls-key-type` arguments , `tls-identity` ou `tls-cipher` pour afficher uniquement les contrôleurs ayant ces attributs TLS :

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Informations associées

- "sous-système nvme vserver"

Désactivation du canal sécurisé TLS pour NVMe/TCP

À partir de ONTAP 9.16.1, vous pouvez configurer le canal sécurisé TLS pour les connexions NVMe/TCP. Si vous avez configuré un canal sécurisé TLS pour les connexions NVMe/TCP, vous pouvez choisir de le désactiver à tout moment.

Étapes

1. Supprimez l'hôte du sous-système pour désactiver le canal sécurisé TLS :

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Vérifiez que le canal sécurisé TLS est supprimé de l'hôte :

```
vserver nvme subsystem host show
```

3. Ajoutez de nouveau l'hôte au sous-système sans canal sécurisé TLS :

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Informations associées

- "hôte du sous-système nvme vserver"

Modification de la priorité d'hôte NVMe

À partir de ONTAP 9.14.1, vous pouvez configurer votre sous-système NVMe de manière à hiérarchiser l'allocation des ressources pour des hôtes spécifiques. Par défaut, lorsqu'un hôte est ajouté au sous-système, il se voit attribuer une priorité régulière. Les hôtes affectés à une priorité élevée reçoivent un nombre de files d'attente d'E/S et des profondeurs de files d'attente plus importants.

Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour modifier manuellement la priorité par défaut, de normal à élevée. Pour modifier la priorité attribuée à un hôte, vous devez supprimer l'hôte du sous-système, puis l'ajouter à nouveau.

Étapes

1. Vérifiez que la priorité de l'hôte est définie sur Normal :

```
vserver nvme show-host-priority
```

Pour en savoir plus, `vserver nvme show-host-priority` consultez le "Référence de commande

ONTAP".

2. Supprimez l'hôte du sous-système :

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Pour en savoir plus, `vserver nvme subsystem host remove` consultez le "Référence de commande ONTAP".

3. Vérifiez que l'hôte est supprimé du sous-système :

```
vserver nvme subsystem host show
```

Pour en savoir plus, `vserver nvme subsystem host show` consultez le "Référence de commande ONTAP".

4. Ajoutez de nouveau l'hôte au sous-système avec une priorité élevée :

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Pour en savoir plus, `vserver nvme subsystem host add` consultez le "Référence de commande ONTAP".

Gérez la détection automatisée d'hôtes de contrôleurs NVMe/TCP dans ONTAP

Depuis la version ONTAP 9.14.1, la détection des contrôleurs hôtes utilisant le protocole NVMe/TCP est automatisée par défaut dans les fabrics basés sur IP.

Activez la détection automatisée d'hôtes des contrôleurs NVMe/TCP

Si vous avez précédemment désactivé la découverte automatique d'hôtes, mais que vos besoins ont changé, vous pouvez la réactiver.

Étapes

1. Entrer en mode de privilège avancé :

```
set -privilege advanced
```

2. Activer la découverte automatisée :

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Vérifiez que la détection automatisée des contrôleurs NVMe/TCP est activée.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Désactivation de la découverte automatique d'hôtes des contrôleurs NVMe/TCP

Si votre hôte n'a pas besoin de détecter automatiquement les contrôleurs NVMe/TCP et que vous détectez le trafic multidiffusion indésirable sur votre réseau, désactivez cette fonctionnalité.

Étapes

1. Entrer en mode de privilège avancé :

```
set -privilege advanced
```

2. Désactiver la découverte automatique :

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Vérifiez que la détection automatisée des contrôleurs NVMe/TCP est désactivée.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Désactivez l'identificateur de machine virtuelle hôte NVMe dans ONTAP

Depuis la version ONTAP 9.14.1, par défaut, ONTAP prend en charge la possibilité pour les hôtes NVMe/FC d'identifier les machines virtuelles à l'aide d'un identifiant unique, et pour les hôtes NVMe/FC de surveiller l'utilisation des ressources des machines virtuelles. Cela améliore le reporting et la résolution des problèmes côté hôte.

Vous pouvez utiliser le bootarg pour désactiver cette fonctionnalité.

Étape

1. Désactiver l'identifiant de la machine virtuelle :

```
bootargs set fct_sli_appid_off <port>, <port>
```

L'exemple suivant désactive le VMID sur le port 0g et le port 0i.

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

Gestion des systèmes avec les adaptateurs FC

Gestion des systèmes avec les adaptateurs FC

Des commandes sont disponibles pour la gestion des adaptateurs FC intégrés et des cartes d'adaptateur FC. Ces commandes peuvent être utilisées pour configurer le mode adaptateur, afficher les informations relatives à l'adaptateur et modifier la vitesse.

La plupart des systèmes de stockage disposent d'adaptateurs FC intégrés qui peuvent être configurés comme initiateurs ou cibles. Vous pouvez également utiliser des cartes adaptateurs FC configurées comme initiateurs ou cibles. Les initiateurs se connectent aux étagères de disques principales et éventuellement aux baies de stockage étrangères. Les cibles se connectent uniquement aux commutateurs FC. Les ports HBA cibles FC et la vitesse du port du commutateur doivent être définis sur la même valeur et ne doivent pas être définis sur automatique.

Informations associées

"Configuration SAN"

Commandes de gestion des adaptateurs FC

Vous pouvez utiliser des commandes FC pour gérer les adaptateurs cibles FC, les adaptateurs initiateurs FC et les adaptateurs FC intégrés à votre contrôleur de stockage. Les mêmes commandes sont utilisées pour gérer les adaptateurs FC pour le protocole FC et le protocole FC-NVMe.

Les commandes de l'adaptateur initiateur FC fonctionnent uniquement au niveau du nœud. Vous devez utiliser le `run -node *node_name*` Commande avant de pouvoir utiliser les commandes de l'adaptateur FC initiator.

Commandes de gestion des adaptateurs cibles FC

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche les informations relatives à l'adaptateur FC sur un nœud	`network fcp adapter show`
Modifiez les paramètres de l'adaptateur cible FC	`network fcp adapter modify`
Affiche les informations de trafic du protocole FC	`run -node *node_name* sysstat -f`
Afficher la durée d'exécution du protocole FC	`run -node *node_name* uptime`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche la configuration et l'état de la carte	`run -node node_name sysconfig -v adapter`
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	`run -node node_name sysconfig -ac`
Affichez une page man pour une commande	`man <command_name>`

Commandes de gestion des adaptateurs initiateurs FC

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche les informations relatives à la totalité des initiateurs et de leurs adaptateurs dans un nœud	`run -node node_name storage show adapter`
Affiche la configuration et l'état de la carte	`run -node node_name sysconfig -v adapter`
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	`run -node node_name sysconfig -ac`

Commandes de gestion des adaptateurs FC intégrés

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche l'état des ports FC intégrés	`run -node node_name system hardware unified-connect show`

Informations associées

- "adaptateur réseau fcp"

Configurez les adaptateurs FC

Chaque port FC intégré peut être configuré individuellement en tant qu'initiateur ou cible. Les ports de certains adaptateurs FC peuvent également être configurés individuellement en tant que port cible ou port initiateur, comme les ports FC intégrés. Une liste d'adaptateurs pouvant être configurés pour le mode cible est disponible dans le "NetApp Hardware Universe".

Le mode cible est utilisé pour connecter les ports aux initiateurs FC. Le mode initiateur permet de connecter les ports aux lecteurs de bande, aux bibliothèques de bandes ou aux systèmes de stockage tiers via l'importation de LUN étrangers (FLI).

La même procédure est utilisée lors de la configuration des adaptateurs FC pour le protocole FC et le protocole FC-NVMe. Cependant, seuls certains adaptateurs FC prennent en charge la connectivité FC-NVMe. Voir la "NetApp Hardware Universe" Par l'utilisation de la liste des adaptateurs prenant en charge le protocole

FC-NVMe.

Configurer les adaptateurs FC pour le mode cible

Étapes

1. Mettez l'adaptateur hors ligne :

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

2. Modifiez l'adaptateur de l'initiateur sur la cible :

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.
4. Vérifiez que la configuration du port cible est correcte :

   ```
   network fcp adapter show -node node_name
   ```

   Pour en savoir plus, `network fcp adapter show` consultez le "Référence de commande ONTAP".

5. Mettez votre adaptateur en ligne :

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

Configurer les adaptateurs FC pour le mode initiateur

Avant de commencer

- Les LIF présentes sur l'adaptateur doivent être supprimées de n'importe quel ensemble de ports dont elles sont membres.
- Toutes les LIF de chaque machine virtuelle de stockage (SVM) utilisant le port physique à modifier doivent être migrées ou détruites avant de changer la personnalité du port physique de la cible à l'initiateur.

> Le protocole NVMe/FC prend en charge le mode initiateur.

Étapes

1. Supprimer toutes les LIFs de l'adaptateur :

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

   Pour en savoir plus, `network interface delete` consultez le "Référence de commande ONTAP".

2. Mettez votre adaptateur hors ligne :

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Modifiez l'adaptateur de la cible à l'initiateur :

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.
5. Vérifier que les ports FC sont configurés dans l'état approprié pour votre configuration :

   ```
   system hardware unified-connect show
   ```

6. Remettre la carte en ligne :

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

Afficher les paramètres de la carte

Vous pouvez utiliser des commandes spécifiques pour afficher des informations sur vos adaptateurs FC/UTA.

Adaptateur FC cible

Étape

1. Utilisez le `network fcp adapter show` commande permettant d'afficher les informations relatives à l'adaptateur : `network fcp adapter show -instance -node node1 -adapter 0a`

   Le résultat de cette commande affiche des informations de configuration du système et des informations sur l'adaptateur pour chaque slot utilisé.

   Pour en savoir plus, `network fcp adapter show` consultez le "Référence de commande ONTAP".

Adaptateur « Unified Target » (UTA) X1143A-R6

Étapes

1. Démarrez votre contrôleur sans les câbles connectés.
2. Exécutez le `system hardware unified-connect show` commande pour afficher la configuration des ports et les modules.
3. Afficher les informations relatives aux ports avant de configurer le CNA et les ports.

Remplacez le port UTA2 du mode CNA par le mode FC

Vous devez modifier le port UTA2 entre le mode CNA (Converged Network adapter) et le mode FC (Fibre Channel) pour prendre en charge l'initiateur FC et le mode cible FC. Vous devez modifier la personnalité du mode CNA en mode FC lorsque vous devez modifier le support physique qui connecte le port à son réseau.

Étapes

1. Mettez l'adaptateur hors ligne :

   ```
   network fcp adapter modify -node node_name -adapter adapter_name -status-admin
   down
   ```

2. Modifiez le mode des ports :

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. Redémarrez le nœud, puis mettez l'adaptateur en ligne :

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. Informez votre administrateur ou votre gestionnaire vif de supprimer ou de supprimer le port, le cas échéant :

   - Si le port est utilisé en tant que port d'origine d'une LIF, est membre d'un groupe d'interface (ifgrp), ou des VLAN hôtes, un administrateur doit faire ce qui suit :

     i. Déplacez les LIF, retirez le port du ifgrp ou supprimez les VLAN.

     ii. Supprimez manuellement le port en exécutant le `network port delete` commande.

     Si le `network port delete` échec de la commande, l'administrateur doit corriger les erreurs, puis exécuter de nouveau la commande.

     Pour en savoir plus, `network port delete` consultez le "Référence de commande ONTAP".

   - Si le port n'est pas utilisé comme port de base d'une LIF, n'est pas membre d'un ifgrp. Il ne héberge pas les VLAN, alors le vif Manager doit supprimer le port de ses enregistrements au moment du redémarrage.

     Si le vif Manager ne supprime pas le port, l'administrateur doit le supprimer manuellement après le redémarrage à l'aide du `network port delete` commande.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter    Mode     Type       Mode     Type
Status
    ------------    -------    -------  ---------  -------  ---------
```

```
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

5. Vérifiez que le SFP+ est installé correctement :

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit ou un SFP 16 Gbit avant de modifier la configuration sur le nœud.

   Pour en savoir plus, `network fcp adapter show` consultez le "Référence de commande ONTAP".

Informations associées

- "interface réseau"

Modifiez les modules optiques des adaptateurs CNA/UTA2

Vous devez modifier les modules optiques de l'adaptateur cible unifié (CNA/UTA2) pour prendre en charge le mode de personnalisation sélectionné pour l'adaptateur.

Étapes

1. Vérifiez le SFP+ actuel utilisé dans la carte. Ensuite, remplacez le SFP+ actuel par le SFP+ approprié pour la personnalité préférée (FC ou CNA).
2. Retirez les modules optiques actuels de l'adaptateur X1143A-R6.
3. Insérez les modules appropriés pour l'optique de votre mode de personnalisation préféré (FC ou CNA).
4. Vérifiez que le SFP+ est installé correctement :

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Les modules SFP+ et les câbles cuivre (Twinax) de marque Cisco sont répertoriés dans le *Hardware Universe*.

Informations associées

- "NetApp Hardware Universe"
- "network fcp adapter affiche"

Configurations de ports prises en charge pour les adaptateurs X1143A-R6

Le mode FC target est la configuration par défaut pour les ports d'adaptateur X1143A-R6. Cependant, les ports de cet adaptateur peuvent être configurés en tant que ports Ethernet 10 Gb et FCoE ou en tant que ports FC 16 Gb.

Lorsqu'ils sont configurés pour Ethernet et FCoE, les adaptateurs X1143A-R6 prennent en charge le trafic cible FCoE et les cartes réseau simultanés sur le même port 10 GBE. Lorsqu'elle est configurée pour FC, chaque paire à deux ports qui partage le même ASIC peut être configurée individuellement pour le mode FC cible ou initiateur FC. Cela signifie qu'un seul adaptateur X1143A-R6 peut prendre en charge le mode cible FC sur une paire à deux ports et le mode initiateur FC sur une autre paire à deux ports.

Informations associées

"NetApp Hardware Universe"

"Configuration SAN"

Configurez les ports

Pour configurer l'adaptateur cible unifié (X1143A-R6), vous devez configurer les deux ports adjacents sur la même puce dans le même mode de personnalisation.

Étapes

1. Configurez les ports selon vos besoins pour Fibre Channel (FC) ou CNA (Converged Network adapter) à l'aide du `system node hardware unified-connect modify` commande.
2. Connectez les câbles appropriés pour FC ou Ethernet 10 Gbit.
3. Vérifiez que le SFP+ est installé correctement :

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit ou un SFP 16 Gbit, selon la structure FC à laquelle vous êtes connecté.

   Pour en savoir plus, `network fcp adapter show` consultez le "Référence de commande ONTAP".

Prévention des pertes de connectivité avec l'adaptateur X1133A-R6

Vous pouvez éviter la perte de connectivité lors d'une défaillance de port en configurant votre système avec des chemins redondants vers des HBA X1133A-R6 distincts.

La carte HBA X1133A-R6 est un adaptateur FC 16 Gbit à 4 ports composé de deux paires à 2 ports. L'adaptateur X1133A-R6 peut être configuré en mode cible ou initiateur. Chaque paire de 2 ports est prise en charge par un seul ASIC (par exemple, les ports 1 et 2 sur ASIC 1 et les ports 3 et 4 sur ASIC 2). Les deux ports d'un ASIC unique doivent être configurés pour fonctionner dans le même mode, soit en mode cible, soit en mode initiateur. En cas d'erreur sur l'ASIC prenant en charge une paire, les deux ports de la paire sont mis hors ligne.

Pour éviter ce risque de perte de connectivité, vous devez configurer votre système avec des chemins redondants vers des HBA X1133A-R6 distincts, ou avec des chemins redondants vers des ports pris en charge par différents ASIC sur le HBA.

Gérez les LIF de tous les protocoles SAN

Gérez les LIF de tous les protocoles SAN

Les initiateurs doivent utiliser les options MPIO (Multi Path I/O) et ALUA (Asymmetric Logical Unit Access) pour la capacité de basculement des clusters dans un environnement SAN. Si un nœud tombe en panne, les LIFs ne migrent pas et ne partent pas des adresses IP du nœud partenaire défaillant. À la place, le logiciel MPIO, avec ALUA sur l'hôte, est chargé de sélectionner les chemins d'accès appropriés pour les LUN via les LIF.

Vous devez créer un ou plusieurs chemins iSCSI depuis chaque nœud d'une paire haute disponibilité à l'aide des interfaces logiques (LIF) pour permettre l'accès aux LUN qui sont gérés par la paire haute disponibilité. Il est recommandé de configurer une LIF de gestion pour chaque SVM prenant en charge SAN.

La connexion directe ou l'utilisation de commutateurs Ethernet sont prises en charge pour la connectivité. Vous

devez créer des LIF pour les deux types de connectivité.

- Il est recommandé de configurer une LIF de gestion pour chaque SVM prenant en charge SAN. Vous pouvez configurer deux LIF par nœud, un pour chaque structure utilisée avec FC et plusieurs réseaux Ethernet pour iSCSI.

Une fois les LIF créées, elles peuvent être supprimées des jeux de ports, déplacées vers différents nœuds d'une machine virtuelle de stockage (SVM), et supprimées.

Informations associées

- "Configurer la présentation des LIFs"
- "Créer une LIF"

Configurez une LIF NVMe dans ONTAP

Lors de la configuration des LIFs NVMe, certaines exigences doivent être respectées.

Avant de commencer

NVMe doit être pris en charge par l'adaptateur FC sur lequel vous créez la LIF. Les cartes prises en charge sont répertoriées dans le "Hardware Universe".

Description de la tâche

À partir de ONTAP 9.12.1 et versions ultérieures, vous pouvez configurer deux LIF NVMe par nœud sur un maximum de 12 nœuds. Dans ONTAP 9.11.1 et les versions antérieures, vous pouvez configurer deux LIF NVMe par nœud sur un maximum de deux nœuds.

Les règles suivantes s'appliquent lors de la création d'une LIF NVMe :

- NVMe peut être le seul protocole de données sur les LIF de données.
- Vous devez configurer une LIF de gestion pour chaque SVM qui prend en charge SAN.
- Pour ONTAP 9.5 et versions ultérieures, vous devez configurer une LIF NVMe sur le nœud contenant le namespace et sur le partenaire HA du nœud.
- Pour ONTAP 9.4 uniquement :
  - Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
  - Une seule LIF de données NVMe peut être configurée par SVM.

Étapes

1. Créer le LIF :

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

> NVME/TCP est disponible à partir de ONTAP 9.10.1 et versions ultérieures.

2. Vérifier que le LIF a été créé :

```
network interface show -vserver <SVM_name>
```

Après sa création, les LIF NVMe/TCP écoutent la découverte sur le port 8009.

Informations associées

- "interface réseau"

Que savoir avant de déplacer une LIF SAN

Vous n'avez besoin d'effectuer un déplacement de LIF que si vous modifiez le contenu du cluster, par exemple : ajout de nœuds au cluster ou suppression de nœuds. Si vous effectuez un déplacement LIF, vous n'avez pas besoin de remettre votre structure FC ou de créer de nouvelles sessions iSCSI entre les hôtes connectés de votre cluster et la nouvelle interface cible.

Vous ne pouvez pas déplacer une LIF SAN à l'aide de `network interface move` commande. Le déplacement de la LIF SAN doit être effectué en mettant la LIF hors ligne, en la déplaçant vers un autre nœud ou port de rattachement, puis en la remettant en ligne sur son nouvel emplacement. L'ALUA (Asymmetric Logical Unit Access) offre des chemins redondants et une sélection de chemin automatique dans le cadre de n'importe quelle solution SAN de ONTAP. Par conséquent, il n'y a pas d'interruption d'E/S lorsque la LIF est mise hors ligne pour le déplacement. L'hôte tente simplement de retraiter et déplace les E/S vers un autre LIF.

Grâce au déplacement de LIF, vous pouvez effectuer les opérations suivantes sans interruption :

- Remplacez une paire haute disponibilité d'un cluster par une paire haute disponibilité mise à niveau de manière transparente pour les hôtes qui accèdent aux données de la LUN
- Mettre à niveau une carte d'interface cible
- Transfert des ressources d'un serveur virtuel de stockage (SVM) d'un ensemble de nœuds d'un cluster vers un autre ensemble de nœuds du cluster

Supprimer une LIF SAN d'un port set

Si la LIF que vous souhaitez supprimer ou déplacer se trouve dans un port set, vous devez supprimer la LIF du port set avant de pouvoir supprimer ou déplacer la LIF.

Description de la tâche

Vous n'avez à effectuer l'étape 1 que si une LIF est dans le port set. Vous ne pouvez pas supprimer la dernière LIF d'un port défini si l'ensemble de ports est lié à un groupe initiateur. Sinon, vous pouvez commencer par l'étape 2 si plusieurs LIF se trouvent dans le port défini.

Étapes

1. Si un seul LIF est dans le port set, utilisez le `lun igroup unbind` commande permettant de dissocier le port défini sur le groupe initiateur.

> Lorsque vous annulez la liaison d'un groupe initiateur à un ensemble de ports, tous les initiateurs du groupe initiateur ont accès à toutes les LUN cibles mappées sur le groupe initiateur sur toutes les interfaces réseau.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

Pour en savoir plus, `lun igroup unbind` consultez le "Référence de commande ONTAP".

2. Utilisez le `lun portset remove` Commande de supprimer le LIF du port set.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Pour en savoir plus, `lun portset remove` consultez le "Référence de commande ONTAP".

Déplacer une LIF SAN

Si un nœud doit être mis hors ligne, vous pouvez déplacer une LIF SAN afin de préserver ses informations de configuration, telles que son WWPN, et éviter de resegmentation de la structure du commutateur. Comme une LIF SAN doit être mise hors ligne avant de pouvoir être déplacée, le trafic hôte doit utiliser un logiciel de chemins d'accès multiples sur l'hôte pour assurer un accès sans interruption à la LUN. Vous pouvez déplacer des LIF SAN vers n'importe quel nœud d'un cluster, mais vous ne pouvez pas déplacer ces LIF entre des SVM (Storage Virtual machine).

Avant de commencer

Si le LIF est membre d'un port set, il faut que la LIF ait été supprimée du port set avant de pouvoir déplacer la LIF vers un autre nœud.

Description de la tâche

Le nœud de destination et le port physique d'une LIF que vous souhaitez déplacer doivent se trouver sur la même structure FC ou sur un même réseau Ethernet. Si vous déplacez une LIF vers une autre structure qui n'a pas été correctement zonée ou si vous déplacez la LIF vers un réseau Ethernet qui n'a pas de connectivité entre l'initiateur iSCSI et la cible, la LUN sera inaccessible lorsque vous la remettez en ligne.

Étapes

1. Afficher le statut administratif et opérationnel de la LIF :

```
network interface show -vserver vserver_name
```

Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

2. Modifiez le statut de la LIF en `down` (hors ligne) :

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin
down
```

Pour en savoir plus, `network interface modify` consultez le "Référence de commande ONTAP".

3. Assigner le LIF à un nouveau nœud et port :

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node_name -home-port port_name
```

4. Modifiez le statut de la LIF en `up` (en ligne) :

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".

5. Vérifiez les modifications :

```
network interface show -vserver vserver_name
```

Supprimez une LIF dans un environnement SAN

Avant de supprimer une LIF, assurez-vous que l'hôte connecté à la LIF peut accéder aux LUN via un autre chemin.

Avant de commencer

Si la LIF que vous souhaitez supprimer est membre d'un port set, vous devez d'abord supprimer cette LIF du port set avant de pouvoir supprimer la LIF.

System Manager

Supprimez une LIF avec ONTAP System Manager (9.7 et versions ultérieures).

Étapes

1. Dans System Manager, cliquez sur **réseau > Présentation**, puis sélectionnez **interfaces réseau**.
2. Sélectionnez la VM de stockage dont vous souhaitez supprimer la LIF.
3. Cliquez sur ⋮ et sélectionnez **Supprimer**.

CLI

Suppression d'une LIF via l'interface de ligne de commandes de ONTAP

Étapes

1. Vérifier le nom de la LIF et le port actuel à supprimer :

   ```
   network interface show -vserver vserver_name
   ```

2. Supprimez le LIF :

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

   Pour en savoir plus, `network interface delete` consultez le "Référence de commande ONTAP".

3. Vérifier que vous avez supprimé la LIF :

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                     Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

Conditions requises POUR l'ajout de nœuds à un cluster VIA SAN LIF

Lors de l'ajout de nœuds à un cluster, vous devez tenir compte de certaines considérations.

- Vous devez créer des LIF sur les nouveaux nœuds si nécessaire avant de créer des LUN sur ces nouveaux nœuds.
- Vous devez découvrir ces LIF depuis les hôtes, selon la pile hôte et le protocole.
- Vous devez créer des LIF sur les nouveaux nœuds afin que les mouvements de LUN et de volumes soient possibles sans utiliser le réseau d'interconnexion des clusters.

Configurer les LIF iSCSI pour renvoyer le FQDN à l'hôte iSCSI SendTargets Discovery Operation

Depuis ONTAP 9, les LIF iSCSI peuvent être configurées de façon à renvoyer un nom de domaine complet (FQDN) lorsqu'un OS hôte envoie une opération de découverte iSCSI SendTargets. Le retour d'un FQDN est utile lorsqu'il existe un périphérique NAT (Network Address Translation) entre le système d'exploitation hôte et le service de stockage.

Description de la tâche

Les adresses IP d'un côté du périphérique NAT n'ont aucun sens de l'autre côté, mais les FQDN peuvent avoir une signification des deux côtés.

> La limite d'interopérabilité de la valeur FQDN est de 128 caractères sur tous les se hôtes.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Configurer les LIF iSCSI pour renvoyer un FQDN :

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   Dans l'exemple suivant, les LIFs iSCSI sont configurées de renvoyer storagehost-005.example.com en tant que FQDN.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Vérifiez que sendTargets est le FQDN :

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   Dans cet exemple, storagehost-005.example.com s'affiche dans le champ de sortie sendTargets-fqdn.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif        sendtargets-fqdn
------- ---------- --------------------------
vs1     vs1_iscsi1 storagehost-005.example.com
vs1     vs1_iscsi2 storagehost-006.example.com
```

Informations associées

"Référence de commande ONTAP"

Activez l'allocation d'espace ONTAP pour les protocoles SAN

L'allocation d'espace ONTAP vous aide à empêcher la mise hors ligne de vos LUN ou de vos namespaces NVMe en cas d'manque d'espace et permet à vos hôtes SAN de récupérer de l'espace.

La prise en charge de ONTAP pour l'allocation de l'espace dépend de votre protocole SAN et de votre version de ONTAP. Depuis la version ONTAP 9.16.1, l'allocation d'espace est activée par défaut pour les protocoles iSCSI, FC et NVMe pour les nouvelles LUN et tous les espaces de noms.

Version ONTAP	Protocoles	L'allocation d'espace est…
9.16.1 ou ultérieure	• ISCSI • FC • NVMe	Activé par défaut pour les LUN nouvellement créées et tous les namespaces
9.15.1	• ISCSI • FC	Activé par défaut pour les nouvelles LUN créées
	NVMe	Non pris en charge
9.14.1 et versions antérieures	• ISCSI • FC	Désactivé par défaut pour les nouvelles LUN créées
	NVMe	Non pris en charge

Lorsque l'allocation d'espace est activée :

- Si l'espace d'une LUN ou d'un espace de nom est insuffisant, ONTAP communique à l'hôte qu'aucun espace libre n'est disponible pour les opérations d'écriture. Par conséquent, la LUN ou le namespace reste en ligne et les opérations de lecture continuent d'être traitées. Selon la configuration de l'hôte, soit l'hôte réessaie les opérations d'écriture jusqu'à ce qu'elle réussisse, soit le système de fichiers hôte est mis hors ligne. Les opérations d'écriture reprennent lorsque de l'espace libre supplémentaire est disponible pour la LUN ou l'espace de noms.

  Si l'allocation d'espace n'est pas activée, lorsqu'une LUN ou un espace de nom manque d'espace, toutes les opérations d'E/S échouent et la LUN ou l'espace de noms est mis hors ligne. Le problème d'espace doit être résolu pour que les opérations reprennent normalement. Il peut également être nécessaire de

renumériser les périphériques LUN sur l'hôte pour restaurer les chemins et les périphériques à un état opérationnel.

- Un hôte peut effectuer des opérations SCSI ou NVME `UNMAP` (parfois appelées `TRIM`). Les opérations UNMAP permettent à un hôte d'identifier les blocs de données qui ne sont plus nécessaires, car ils ne contiennent plus de données valides. L'identification se produit normalement après la suppression du fichier. Le système de stockage peut ensuite désallouer ces blocs de données afin que l'espace puisse être consommé ailleurs. Cette désallocation améliore considérablement l'efficacité globale du stockage, en particulier avec les systèmes de fichiers dont le volume de données est élevé.

Avant de commencer

L'activation de l'allocation d'espace nécessite une configuration hôte capable de gérer correctement les erreurs d'allocation d'espace lorsqu'une écriture ne peut pas être terminée. L'exploitation de SCSI ou NVME `UNMAP` nécessite une configuration qui peut utiliser le provisionnement de blocs logiques, comme défini dans la norme SCSI SBC-3.

Les hôtes suivants prennent actuellement en charge le provisionnement fin lorsque vous activez l'allocation d'espace :

- Citrix XenServer 6.5 et versions ultérieures
- VMware ESXi 5.0 et versions ultérieures
- Noyau Oracle Linux 6.2 UEK et versions ultérieures
- Red Hat Enterprise Linux 6.2 et versions ultérieures
- SUSE Linux Enterprise Server 11 et versions ultérieures
- Solaris 11.1 et versions ultérieures
- Répertoires de base

Description de la tâche

Lorsque vous mettez à niveau votre cluster vers ONTAP 9.15.1 ou une version ultérieure, le paramètre d'allocation d'espace pour toutes les LUN créées avant la mise à niveau logicielle reste le même après la mise à niveau, quel que soit le type d'hôte. Par exemple, si une LUN a été créée dans ONTAP 9.13.1 pour un hôte VMware dont l'allocation d'espace est désactivée, l'allocation d'espace sur cette LUN reste désactivée après la mise à niveau vers ONTAP 9.15.1.

Étapes

1. Activer l'allocation d'espace :

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Vérifiez que l'allocation d'espace est activée :

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Vérifiez que l'allocation d'espace est activée sur le système d'exploitation hôte.

Certaines configurations hôte, y compris certaines versions de VMware ESXi, peuvent automatiquement reconnaître la modification des paramètres et ne nécessitent pas l'intervention de l'utilisateur. D'autres configurations peuvent nécessiter une nouvelle analyse du périphérique. Certains systèmes de fichiers et gestionnaires de volumes peuvent nécessiter des paramètres spécifiques supplémentaires pour activer la récupération d'espace à l'aide de `SCSI UNMAP`. Le montage des systèmes de fichiers ou le redémarrage complet du système d'exploitation peuvent être nécessaires. Consultez la documentation de votre hôte spécifique pour obtenir de l'aide.

Configuration de l'hôte pour les hôtes VMware ESXi 8.x et les hôtes NVMe ultérieurs

Si vous disposez d'un hôte VMware exécutant ESXi 8.x ou une version ultérieure avec le protocole NVMe, une fois que vous avez activé l'allocation d'espace dans ONTAP, vous devez effectuer les étapes suivantes sur les hôtes.

Étapes

1. Sur votre hôte ESXi, vérifiez que le DSM est désactivé :

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   La valeur attendue est 0.

2. Activez le DSM NVMe :

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. Vérifiez que le DSM est activé :

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   La valeur attendue est 1.

Liens connexes

En savoir plus sur "Configuration hôte NVMe-of pour ESXi 8.x avec ONTAP".

Combinaisons de configuration de volumes et de fichiers ou de LUN recommandées

Présentation des combinaisons de configuration de volumes et fichiers ou LUN recommandées

Il existe des combinaisons spécifiques de configurations de volumes et fichiers FlexVol ou LUN qui peuvent être utilisées, en fonction des exigences de l'application et de l'administration. Connaître les avantages et les coûts de ces combinaisons vous aidera à déterminer la combinaison volume-LUN qui convient à votre environnement.

Les combinaisons de configuration de volume et de LUN suivantes sont recommandées :

- Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd
- Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume
- Fichiers ou LUN réservés en espace avec provisionnement de volumes semi-lourds

Vous pouvez utiliser le provisionnement fin SCSI sur vos LUN en association avec l'une de ces combinaisons de configuration.

Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd

Avantages :

- Toutes les opérations d'écriture dans les fichiers réservés à l'espace sont garanties ; elles ne échoueront pas en raison de l'espace insuffisant.
- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.

Coûts et limitations:

- L'espace doit être suffisant en dehors de l'agrégat pour prendre en charge le volume bénéficiant du provisionnement.
- Un espace égal à deux fois la taille de la LUN est alloué au volume au moment de sa création.

Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume

Avantages :

- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.
- L'espace est alloué uniquement lorsqu'il est utilisé.

Coûts et restrictions:

- Les opérations d'écriture ne sont pas garanties ; elles peuvent échouer si le volume vient à manquer d'espace.
- Vous devez gérer efficacement l'espace libre dans l'agrégat pour empêcher ce dernier de manquer d'espace.

Fichiers ou LUN réservés en espace avec provisionnement de volumes semi-lourds

Avantages :

L'espace réservé est inférieur à celui du provisionnement d'un volume non lourd et la garantie d'écriture optimale est toujours fournie.

Coûts et restrictions:

- Cette option permet d'échouer les opérations d'écriture.

  Vous pouvez réduire ce risque en équilibrant correctement l'espace libre du volume par rapport à la volatilité des données.

- Vous ne pouvez pas vous fier à la conservation des objets de protection des données tels que les snapshots, les fichiers FlexClone et les LUN.
- Vous ne pouvez pas utiliser les fonctionnalités ONTAP d'efficacité du stockage de partage de blocs qui ne peuvent pas être supprimées automatiquement, notamment la déduplication, la compression et ODX/déchargement des copies.

Déterminez la combinaison de configuration de volume et de LUN adaptée à votre environnement

En répondant à quelques questions de base sur votre environnement, vous pourrez déterminer la meilleure configuration de volumes FlexVol et de LUN pour votre environnement.

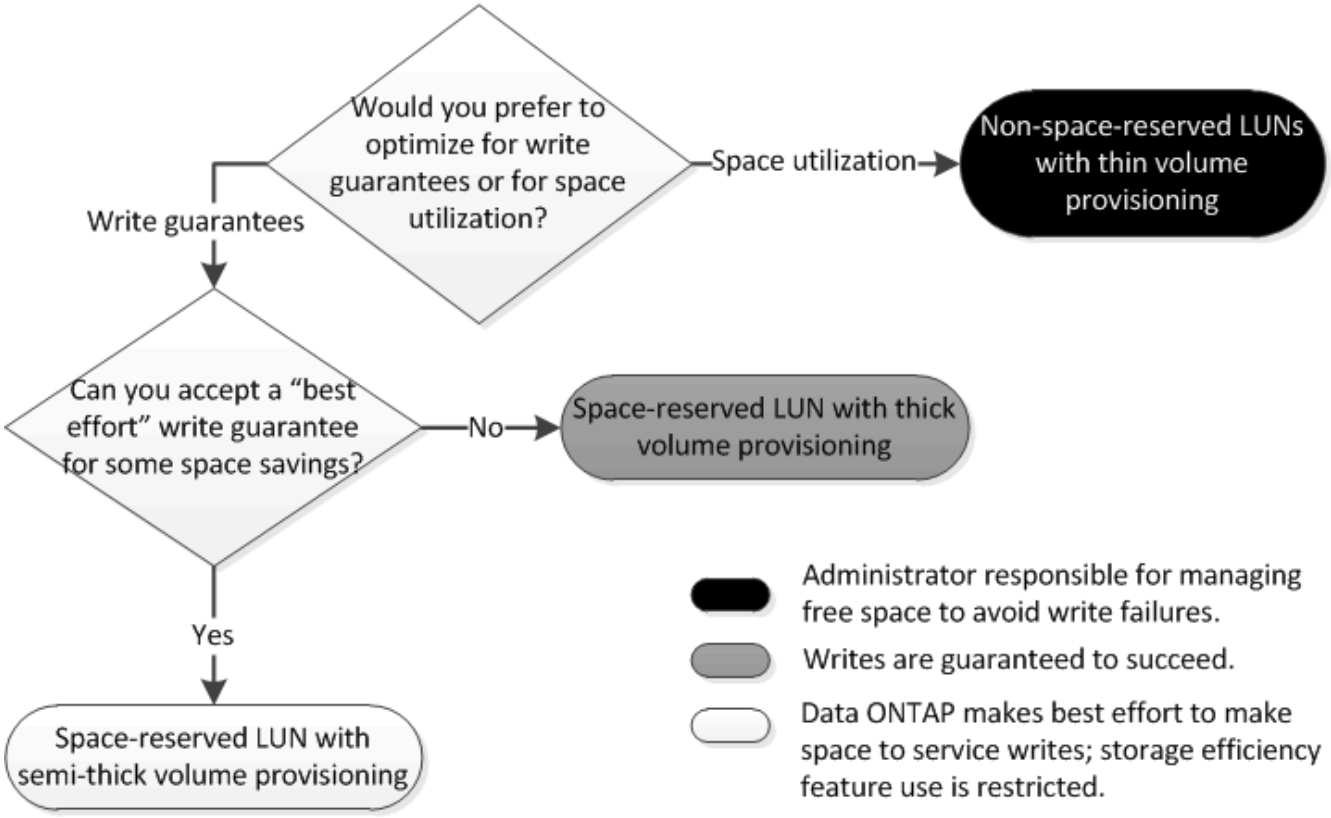
Description de la tâche

Vous pouvez optimiser les configurations des LUN et des volumes pour optimiser l'utilisation du stockage ou pour garantir la sécurité de l'écriture. En fonction de vos besoins en matière d'utilisation du stockage et de votre capacité à surveiller et à assurer la capacité des stocks disponibles rapidement, vous devez déterminer le volume FlexVol et les volumes LUN appropriés à votre installation.

> Aucun volume n'est nécessaire pour chaque LUN.

Étape

1. Utilisez l'arbre de décision suivant pour déterminer la meilleure combinaison de configuration de volumes et de LUN pour votre environnement :



Calculer le taux de croissance des données pour les LUN

Vous devez connaître la vitesse de croissance de vos données LUN afin de déterminer si vous devez utiliser des LUN réservées à l'espace ou des LUN non réservées à l'espace.

Description de la tâche

Si vous taux de croissance des données régulièrement élevé, les LUN réservées à l'espace pourraient vous constituer une meilleure option. Si vous taux de croissance des données est faible, vous devez envisager des LUN non réservées aux espaces.

Vous pouvez utiliser des outils tels que OnCommand Insight pour calculer le taux de croissance de vos données ou le calculer manuellement. Les étapes suivantes concernent le calcul manuel.

Étapes

1. Configurez une LUN Space-Reserved.
2. Surveillez les données de la LUN pendant une période définie, par exemple une semaine.

   Assurez-vous que votre période de surveillance est suffisamment longue pour former un échantillon représentatif des augmentations régulières de la croissance des données. Par exemple, vous pourriez avoir une forte croissance du volume des données de manière cohérente à la fin de chaque mois.

3. Chaque jour, enregistrez en Go la croissance de vos données.
4. À la fin de votre période de surveillance, additionnez les totaux pour chaque jour, puis divisez par le nombre de jours de votre période de surveillance.

   Ce calcul produit votre taux de croissance moyen.

Exemple

Dans cet exemple, vous avez besoin d'une LUN de 200 Go. Vous décidez de contrôler le LUN pendant une semaine et d'enregistrer les modifications quotidiennes suivantes :

- Dimanche : 20 Go
- Lundi: 18 GB
- Mardi: 17 GB
- Mercredi: 20 GB
- Jeudi: 20 GB
- Vendredi : 23 GB
- Samedi: 22 GB

Dans cet exemple, votre taux de croissance est de (20+18+17+20+20+23+22) / 7 = 20 Go par jour.

Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec des volumes à provisionnement lourd

La combinaison de configuration de volume et fichier FlexVol/LUN vous permet d'utiliser des technologies d'efficacité du stockage et ne vous demande pas de surveiller activement votre espace libre, car l'espace est alloué en amont.

Les paramètres suivants sont nécessaires pour configurer un fichier ou une LUN réservé à l'espace dans un volume à l'aide du provisionnement Thick :

Réglage du volume	Valeur
Résultats garantis	Volumétrie
Réserve fractionnaire	100
Réserve Snapshot	Toutes

Réglage du volume	Valeur
Suppression automatique de l'instantané	Facultatif
Croissance automatique	Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé.

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Activé

Paramètres de configuration pour les fichiers ou LUN non réservés en espace avec des volumes à provisionnement fin

Cette combinaison de configuration de volumes et de fichiers FlexVol ou de LUN requiert la réduction de la quantité de stockage allouée à l'avance, mais elle exige une gestion de l'espace libre actif pour éviter les erreurs liées au manque d'espace.

Les paramètres suivants sont requis pour configurer un LUN ou des fichiers non réservés en espace dans un volume à provisionnement fin :

Réglage du volume	Valeur
Résultats garantis	Aucune
Réserve fractionnaire	0
Réserve Snapshot	Toutes
Suppression automatique de l'instantané	Facultatif
Croissance automatique	Facultatif

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Désactivé

Autres considérations

Lorsque l'espace est insuffisant pour le volume ou l'agrégat, les opérations d'écriture sur le fichier ou la LUN peuvent échouer.

Pour ne pas contrôler activement l'espace disponible pour le volume et l'agrégat, vous devez activer la croissance automatique du volume et définir la taille maximale du volume sur la taille de l'agrégat. Dans cette configuration, vous devez surveiller activement l'espace libre des agrégats, mais il n'est pas nécessaire de surveiller l'espace libre dans le volume.

Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec provisionnement de volumes semi-lourds

Cette combinaison de configuration de volumes et de fichiers FlexVol ou de LUN requiert moins de stockage que la combinaison entièrement provisionnée, mais impose des restrictions sur les technologies d'efficacité que vous pouvez utiliser pour ce volume. Les écrasements sont effectués par le meilleur effort pour cette combinaison de configuration.

Les paramètres suivants sont nécessaires pour configurer une LUN Space-Reserved dans un volume à l'aide du provisionnement semi-thick :

Réglage du volume	Valeur
Résultats garantis	Volumétrie
Réserve fractionnaire	0
Réserve Snapshot	0
Suppression automatique de l'instantané	On, avec un niveau d'engagement de destruction, une liste de destruction qui inclut tous les objets, le déclencheur défini sur volume, ainsi que toutes les LUN FlexClone et tous les fichiers FlexClone activés pour la suppression automatique.
Croissance automatique	Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé.

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Activé

Restrictions technologiques

Pour cette combinaison de configuration, vous ne pouvez pas utiliser les technologies suivantes d'efficacité du stockage de volumes :

- Compression
- Déduplication
- ODX et allègement de la charge des copies FlexClone
- LUN FlexClone et fichiers FlexClone non marqués pour la suppression automatique (clones actifs)
- Sous-fichiers FlexClone
- ODX/allègement de la charge des copies

Autres considérations

Lors de l'utilisation de cette combinaison de configuration, vous devez tenir compte des éléments suivants :

- Lorsque l’espace d’espace du volume qui prend en charge cette LUN est faible, les données de protection (LUN et fichiers FlexClone, snapshots) sont détruites.
- Les opérations d’écriture peuvent entraîner un temps d’attente et l’échec lorsque l’espace disponible est insuffisant.

Par défaut, la compression est activée pour les plateformes AFF. Vous devez désactiver explicitement la compression pour tout volume pour lequel vous souhaitez utiliser un provisionnement semi-lourd sur une plateforme AFF.

Protection des données SAN

En savoir plus sur les méthodes de protection des données ONTAP pour les environnements SAN

Vous pouvez protéger vos données en les faisant des copies afin qu’elles soient disponibles à des fins de restauration en cas de suppression accidentelle, de panne d’application, de corruption des données ou d’incident. Selon vos besoins en termes de protection et de sauvegarde des données, ONTAP propose plusieurs méthodes pour protéger vos données.

Synchronisation active SnapMirror

Depuis la disponibilité générale de ONTAP 9.9.1, assure un délai de restauration nul ou un basculement transparent des applications (TAF) pour permettre le basculement automatique des applications stratégiques dans les environnements SAN. La synchronisation active SnapMirror nécessite l’installation du logiciel ONTAP Mediator 1.2 dans une configuration comprenant deux clusters AFF ou deux clusters ASA.

"Synchronisation active SnapMirror"

Snapshot

Vous permet de créer, de planifier et de gérer manuellement ou automatiquement plusieurs sauvegardes de vos LUN. Les snapshots n’utilisent qu’une quantité minimale d’espace de volume supplémentaire et n’ont pas de coût pour les performances. En cas de modification ou de suppression accidentelle des données de votre LUN, vous pouvez restaurer ces données facilement et rapidement à partir de l’un des derniers snapshots.

LUN FlexClone (licence FlexClone requise)

Copies inscriptibles à un point dans le temps d’une autre LUN dans un volume actif ou dans un snapshot. Un clone et son parent peuvent être modifiés de façon indépendante sans affecter les autres

SnapRestore (licence requise)

Restauration rapide et compacte des données à partir de copies Snapshot sur un volume entier, sur demande. Vous pouvez utiliser SnapRestore pour restaurer une LUN à un état conservé antérieur sans redémarrer le système de stockage.

Copies miroir de protection des données (licence SnapMirror requise)

Permet une reprise après incident asynchrone en vous permettant de créer régulièrement des snapshots des données sur votre volume, de les copier sur un réseau local ou étendu vers un volume partenaire, généralement sur un autre cluster, et de conserver ces snapshots. La copie miroir du volume partenaire assure

une disponibilité et une restauration rapides des données de l'heure du dernier snapshot, en cas de corruption ou de perte des données du volume source.

Sauvegardes SnapVault (licence SnapMirror requise)

Permet un stockage efficace et une conservation à long terme des sauvegardes. Les relations SnapVault vous permettent de sauvegarder des snapshots sélectionnés de volumes sur un volume de destination et de conserver les sauvegardes.

Si vous réalisez des sauvegardes sur bande et des opérations d'archivage, vous pouvez les effectuer sur les données déjà sauvegardées sur le volume secondaire de SnapVault.

SnapDrive pour Windows ou UNIX (licence SnapDrive requise)

Configure l'accès aux LUN, gère les LUN et gère les snapshots du système de stockage directement à partir d'hôtes Windows ou UNIX.

Sauvegarde et restauration natives sur bande

La prise en charge de la plupart des lecteurs de bandes existants est incluse dans ONTAP, ainsi qu'une méthode permettant aux fournisseurs de bandes d'ajouter dynamiquement la prise en charge des nouveaux périphériques. ONTAP prend également en charge le protocole RMT (Remote Magnetic Tape), permettant ainsi une sauvegarde et une restauration vers tout système capable.

Informations associées

"Documentation NetApp : SnapDrive pour UNIX" "Documentation NetApp : SnapDrive pour Windows (versions actuelles)" "Protection des données par sauvegarde sur bandes"

Restaurer une LUN unique à partir d'une copie Snapshot de ONTAP

Vous pouvez restaurer une seule LUN à partir d'un snapshot sans restaurer l'intégralité du volume qui contient la même LUN. Vous pouvez restaurer la LUN sur place ou sur un nouveau chemin d'accès dans le volume. L'opération restaure uniquement la LUN sans affecter les autres fichiers ou LUN du volume. Vous pouvez également restaurer des fichiers avec des flux.

Avant de commencer

- Vous devez disposer d'espace suffisant sur votre volume pour mener à bien l'opération de restauration :
  - Si vous restaurez une LUN réservée à l'espace où la réserve fractionnaire est 0 %, vous devez avoir une fois la taille de la LUN restaurée.
  - Si vous restaurez une LUN réservée à l'espace où la réserve fractionnaire est de 100 %, vous avez besoin de deux fois la taille de la LUN restaurée.
  - Si vous restaurez une LUN non réservée à l'espace, seul l'espace utilisé pour la LUN restaurée est nécessaire.
- Un snapshot de la LUN de destination doit avoir été créé.

  Si l'opération de restauration échoue, la LUN de destination peut être tronquée. Dans ce cas, vous pouvez utiliser la copie Snapshot pour éviter la perte de données.

- Un snapshot de la LUN source doit avoir été créé.

Dans de rares cas, la restauration de LUN peut échouer, ce qui laisse la LUN source inutilisable. Si cela se produit, vous pouvez utiliser le snapshot pour rétablir l'état de la LUN juste avant la tentative de restauration.

- La LUN de destination et la LUN source doivent avoir le même type de système d'exploitation.

  Si votre LUN de destination possède un type de système d'exploitation différent de votre LUN source, votre hôte peut perdre l'accès aux données à la LUN de destination après l'opération de restauration.

Étapes

1. Depuis l'hôte, arrêtez l'ensemble de l'accès des hôtes au LUN.
2. Démontez la LUN sur son hôte de manière à ce que l'hôte ne puisse pas accéder à la LUN.
3. Annulez le mappage de la LUN :

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. Déterminez le snapshot vers lequel vous souhaitez restaurer la LUN :

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Créez un snapshot de la LUN avant de restaurer la LUN :

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. Restaurer la LUN spécifiée dans un volume :

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. Suivez les étapes à l'écran.
8. Si nécessaire, mettre la LUN en ligne :

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. Si nécessaire, remappage la LUN :

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. Depuis l'hôte, remontez la LUN.
11. Depuis l'hôte, redémarrez l'accès au LUN.

Restaurer toutes les LUN d'un volume à partir d'un snapshot ONTAP

Vous pouvez utiliser `volume snapshot restore` la commande pour restaurer toutes les LUN d'un volume spécifié à partir d'un snapshot.

Étapes

1. Depuis l'hôte, arrêtez l'ensemble de l'accès des hôtes aux LUN.

   L'utilisation de SnapRestore sans interrompre tout accès des hôtes aux LUN du volume peut entraîner une corruption des données et des erreurs système.

2. Démontez les LUN de cet hôte, de sorte que l'hôte ne puisse pas accéder aux LUN.
3. Annulez le mappage de vos LUN :

   ```
   lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
   <lun_name> -igroup <igroup_name>
   ```

4. Déterminez l'instantané vers lequel vous souhaitez restaurer votre volume :

   ```
   volume snapshot show -vserver <SVM_name> -volume <volume_name>
   ```

5. Définissez votre paramètre de privilège sur Avancé :

   ```
   set -privilege advanced
   ```

6. Restaurez vos données :

   ```
   volume snapshot restore -vserver <SVM_name> -volume <volume_name>
   -snapshot <snapshot_name>
   ```

7. Suivez les instructions à l'écran.
8. Remappage de vos LUN :

   ```
   lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
   <lun_name> -igroup <igroup_name>
   ```

9. Vérifiez que vos LUN sont en ligne :

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. Si vos LUN ne sont pas en ligne, mettre-les en ligne :

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. Modifiez votre paramètre de privilège sur admin :

```
set -privilege admin
```

12. A partir de l'hôte, remontez vos LUN.
13. Depuis l'hôte, redémarrez l'accès à vos LUN.

Protégez vos données avec des LUN ONTAP FlexClone

Une LUN FlexClone est une copie inscriptible instantanée d'une autre LUN dans un volume actif ou un snapshot. Le clone et son parent peuvent être modifiés de façon indépendante sans affecter les uns les autres.

Vous pouvez utiliser des LUN FlexClone pour créer plusieurs copies en lecture/écriture d'une LUN.

Raisons de créer des LUN FlexClone

- Vous devez créer une copie temporaire d'une LUN afin d'y effectuer des tests.
- Vous devez mettre une copie de vos données à la disposition d'autres utilisateurs sans pour autant avoir accès aux données de production.
- Vous souhaitez créer un clone de base de données pour les opérations de manipulation et de projection, tout en préservant les données d'origine sous une forme non modifiée.
- Vous souhaitez accéder à un sous-ensemble spécifique des données d'une LUN (un volume logique ou un système de fichiers spécifique dans un groupe de volumes, Ou un fichier spécifique ou un ensemble de fichiers dans un système de fichiers) et copiez-le dans la LUN d'origine, sans restaurer le reste des données de la LUN d'origine. Ce fonctionnement fonctionne sur les systèmes d'exploitation qui prennent en charge le montage simultané d'une LUN et d'un clone de la LUN. SnapDrive pour UNIX en est capable avec le `snap connect` commande.
- Vous avez besoin de plusieurs hôtes de démarrage SAN avec le même système d'exploitation.

Une LUN FlexClone partage initialement de l'espace avec la LUN parent. Par défaut, la LUN FlexClone hérite de l'attribut réservé d'espace de la LUN parent. Par exemple, si la LUN parent est non-réservée à l'espace, la LUN FlexClone est également non réservée à l'espace par défaut. Cependant, vous pouvez créer une LUN FlexClone non réservée à l'espace à partir d'un parent qui est une LUN réservée à l'espace.

Lorsque vous clonez une LUN, le partage de blocs a lieu en arrière-plan et vous ne pouvez pas créer de snapshot de volume tant que le partage de bloc n'est pas terminé.

Vous devez configurer le volume pour activer la fonction de suppression automatique de LUN FlexClone avec `volume snapshot autodelete modify` commande. Sinon, si vous souhaitez que les LUN FlexClone soient supprimées automatiquement, mais que le volume n'est pas configuré pour la suppression automatique

FlexClone, aucune des LUN FlexClone n'est supprimée.

Lorsque vous créez une LUN FlexClone, la fonction de suppression automatique de LUN FlexClone est désactivée par défaut. Vous devez l'activer manuellement sur chaque LUN FlexClone avant de pouvoir supprimer automatiquement cette LUN. Si vous utilisez le provisionnement de volumes semi-lourds et que vous souhaitez la garantie d'écriture « meilleur effort » fournie par cette option, vous devez mettre des LUN *All* FlexClone à disposition pour la suppression automatique.

> Lorsque vous créez une LUN FlexClone à partir d'un snapshot, celle-ci est automatiquement fractionnée de la copie Snapshot à l'aide d'un processus d'arrière-plan compact afin que la LUN ne continue pas à dépendre du snapshot ni à consommer de l'espace supplémentaire. Si ce fractionnement en arrière-plan n'est pas terminé et que ce snapshot est automatiquement supprimé, cette LUN FlexClone est supprimée même si vous avez désactivé la fonction de suppression automatique FlexClone pour cette LUN FlexClone. Une fois la répartition en arrière-plan terminée, la LUN FlexClone n'est pas supprimée, même si l'instantané est supprimé.

Informations associées

- "Créer une LUN FlexClone"
- "Configurez une FlexVol volume pour supprimer automatiquement les LUN FlexClone"
- "Empêche la suppression automatique d'une LUN FlexClone"

Configuration et utilisation des sauvegardes SnapVault dans un environnement SAN

Découvrez les sauvegardes ONTAP SnapVault dans un environnement SAN

La configuration et l'utilisation de SnapVault dans un environnement SAN sont très similaires à celles utilisées dans un environnement NAS. Toutefois, la restauration des LUN dans un environnement SAN nécessite des procédures spéciales.

Les sauvegardes SnapVault contiennent un ensemble de copies en lecture seule d'un volume source. Dans un environnement SAN, vous devez toujours sauvegarder des volumes entiers sur le volume secondaire SnapVault, et non sur des LUN individuelles.

La procédure de création et d'initialisation de la relation SnapVault entre un volume primaire contenant des LUN et un volume secondaire agissant comme sauvegarde SnapVault est identique à la procédure utilisée avec les volumes FlexVol utilisés pour les protocoles de fichiers. Cette procédure est décrite en détail dans "La protection des données".

Il est important de s'assurer que les LUN en cours de sauvegarde sont dans un état cohérent avant la création et la copie des snapshots sur le volume secondaire SnapVault. Grâce à l'automatisation de la création de snapshots avec SnapCenter, les LUN sauvegardées sont complètes et utilisables par l'application d'origine.

Il existe trois options de base pour la restauration des LUN à partir d'un volume secondaire SnapVault :

- Vous pouvez mapper une LUN directement à partir du volume secondaire SnapVault et connecter un hôte au LUN pour accéder au contenu de la LUN.

  La LUN est en lecture seule et vous ne pouvez effectuer un mappage qu'à partir du snapshot le plus récent de la sauvegarde SnapVault. Les réservations et autres métadonnées LUN sont perdues. Si vous le souhaitez, vous pouvez utiliser un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine si celle-ci est toujours accessible.

Le numéro de série de la LUN source est différent de celui de la LUN source.

- Vous pouvez cloner n'importe quel snapshot du volume secondaire SnapVault vers un nouveau volume en lecture-écriture.

  Vous pouvez ensuite mapper l'une des LUN du volume et connecter un hôte au LUN pour accéder au contenu de la LUN. Si vous le souhaitez, vous pouvez utiliser un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine si celle-ci est toujours accessible.

- Vous pouvez restaurer la totalité du volume contenant la LUN à partir de n'importe quel snapshot du volume secondaire SnapVault.

  La restauration du volume entier remplace toutes les LUN, ainsi que tous les fichiers, dans le volume. Toute nouvelle LUN créée depuis la création du Snapshot est perdue.

  Les LUN conservent leur mappage, leur numéro de série, leurs UUID et leurs réservations permanentes.

Accédez à une copie LUN en lecture seule à partir d'une sauvegarde ONTAP SnapVault

Vous pouvez accéder à une copie en lecture seule d'une LUN à partir du dernier snapshot d'une sauvegarde SnapVault. L'ID, le chemin et le numéro de série de la LUN source sont différents de celui-ci et doivent d'abord être mappés. Les réservations permanentes, les mappages de LUN et les groupes initiateurs ne sont pas répliqués sur le volume secondaire SnapVault.

Avant de commencer

- La relation SnapVault doit être initialisée et le dernier snapshot du volume secondaire SnapVault doit contenir la LUN souhaitée.
- Le serveur virtuel de stockage (SVM) contenant la sauvegarde SnapVault doit disposer d'une ou plusieurs LIF avec le protocole SAN souhaité accessible depuis l'hôte utilisé pour accéder à la copie LUN.
- Si vous prévoyez d'accéder directement aux copies de LUN à partir du volume secondaire SnapVault, vous devez créer vos groupes initiateurs sur la SVM SnapVault à l'avance.

  Vous pouvez accéder à une LUN directement à partir du volume secondaire SnapVault sans avoir à effectuer au préalable la restauration ou le clonage du volume contenant la LUN.

Description de la tâche

Si un nouvel instantané est ajouté au volume secondaire SnapVault alors qu'une LUN est mappée à partir d'un snapshot précédent, le contenu de la LUN mappée change. La LUN est toujours mappée avec les mêmes identifiants, mais les données sont extraites du nouveau snapshot. Si la taille de LUN change, certains hôtes détectent automatiquement la modification de taille ; les hôtes Windows exigent une nouvelle analyse du disque pour identifier toute modification de taille.

Étapes

1. Répertorie les LUN disponibles dans le volume secondaire SnapVault.

   ```
   lun show
   ```

   Dans cet exemple, vous pouvez voir les LUN d'origine dans le volume primaire srcvolA et les copies dans

le volume secondaire SnapVault dstvolB :

```
cluster::> lun show

Vserver   Path                  State   Mapped   Type          Size
--------  ------------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

Pour en savoir plus, `lun show` consultez le "Référence de commande ONTAP".

2. Si le groupe initiateur de l'hôte souhaité n'existe pas déjà sur le SVM contenant le volume secondaire SnapVault, créez un groupe initiateur.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

Cette commande crée un groupe initiateur pour un hôte Windows qui utilise le protocole iSCSI :

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Mappez la copie de LUN souhaitée sur le groupe initiateur.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

Pour en savoir plus, `lun mapping create` consultez le "Référence de commande ONTAP".

4. Connectez l'hôte au LUN et accédez au contenu du LUN selon vos besoins.

Restaurer une LUN unique à partir d'une sauvegarde ONTAP SnapVault

Vous pouvez restaurer une seule LUN à un nouvel emplacement ou à l'emplacement d'origine. Vous pouvez effectuer une restauration à partir de n'importe quel snapshot du volume secondaire SnapVault. Pour restaurer la LUN à l'emplacement d'origine, vous devez d'abord la restaurer à un nouvel emplacement, puis la copier.

Avant de commencer

- La relation SnapVault doit être initialisée et le volume secondaire SnapVault doit contenir un snapshot approprié à restaurer.
- La machine virtuelle de stockage (SVM) contenant le volume secondaire SnapVault doit disposer d'une ou plusieurs LIF avec le protocole SAN souhaité accessible depuis l'hôte utilisé pour accéder à la copie de LUN.
- Les igroups doivent déjà exister sur le SVM SnapVault.

Description de la tâche

Le processus comprend la création d'un clone de volume en lecture-écriture à partir d'un snapshot dans le volume secondaire SnapVault. Vous pouvez utiliser la LUN directement depuis le clone ou copier le contenu de la LUN vers l'emplacement d'origine.

Le chemin d'accès et le numéro de série de la LUN d'origine sont différents de ceux de la LUN d'origine. Les réservations permanentes ne sont pas conservées.

Étapes

1. Vérifiez le volume secondaire contenant la sauvegarde SnapVault.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type  Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

2. Identifiez le snapshot à partir duquel vous souhaitez restaurer la LUN.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                      State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Créez un clone en lecture/écriture à partir du snapshot de votre choix

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

Le clone de volume est créé dans le même agrégat que la sauvegarde SnapVault. L'espace doit être suffisant dans l'agrégat pour stocker le clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Répertorier les LUN dans le clone de volume.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

Pour en savoir plus, `lun show` consultez le "Référence de commande ONTAP".

5. Si le groupe initiateur de l'hôte souhaité n'existe pas déjà sur le SVM contenant la sauvegarde SnapVault, créez un groupe initiateur.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

Cet exemple crée un groupe initiateur pour un hôte Windows qui utilise le protocole iSCSI :

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Mappez la copie de LUN souhaitée sur le groupe initiateur.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

Pour en savoir plus, `lun mapping create` consultez le "Référence de commande ONTAP".

7. Connectez l'hôte au LUN et accédez au contenu du LUN, si nécessaire.

   La LUN est en lecture/écriture et peut être utilisée à la place de la LUN d'origine. Le numéro de série de la LUN est différent, l'hôte l'interprète comme une LUN différente de l'original.

8. Utilisez un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine.

Informations associées

- "spectacle snapmirror"

Restaurer toutes les LUN d'un volume à partir d'une sauvegarde ONTAP SnapVault

Si une ou plusieurs LUN d'un volume doivent être restaurées à partir d'une sauvegarde SnapVault, vous pouvez restaurer l'ensemble du volume. La restauration du volume affecte toutes les LUN du volume.

Avant de commencer

La relation SnapVault doit être initialisée et le volume secondaire SnapVault doit contenir un snapshot approprié à restaurer.

Description de la tâche

La restauration d'un volume entier ramène le volume à l'état dans lequel il était au moment de la création de l'instantané. Si une LUN a été ajoutée au volume après le snapshot, cette LUN est supprimée lors du processus de restauration.

Après la restauration du volume, les LUN restent mappées sur les groupes initiateurs auxquels ils ont été

mappés avant la restauration. Le mappage de LUN peut être différent du mappage au moment du snapshot. Les réservations persistantes sur les LUN à partir des clusters hôtes sont conservées.

Étapes

1. Arrêtez les E/S à toutes les LUN du volume.
2. Vérifiez le volume secondaire qui contient le volume secondaire SnapVault.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

3. Identifiez l'instantané à partir duquel vous souhaitez restaurer.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Spécifiez le snapshot à utiliser.

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

La destination que vous spécifiez pour la restauration est le volume d'origine vers lequel vous restaurez.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Si vous partagez des LUN sur un cluster hôte, restaurez les réservations permanentes sur les LUN à partir des hôtes affectés.

Restauration d'un volume à partir d'une sauvegarde SnapVault

Dans l'exemple suivant, la LUN nommée LUN_D a été ajoutée au volume après la création du snapshot. Après la restauration du volume entier à partir du snapshot, lun_D n'apparaît plus.

Dans le `lun show` Résultat de la commande, vous pouvez voir les LUN dans le volume primaire srcvolA et les copies en lecture seule de ces LUN dans le volume secondaire SnapVault dstvolB. Il n'y a pas de copie de lun_D dans la sauvegarde SnapVault.

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

Une fois le volume restauré à partir du volume secondaire SnapVault, le volume source ne contient plus lun_D. Il n'est pas nécessaire de remapper les LUN du volume source une fois la restauration effectuée, car ces LUN restent mappées.

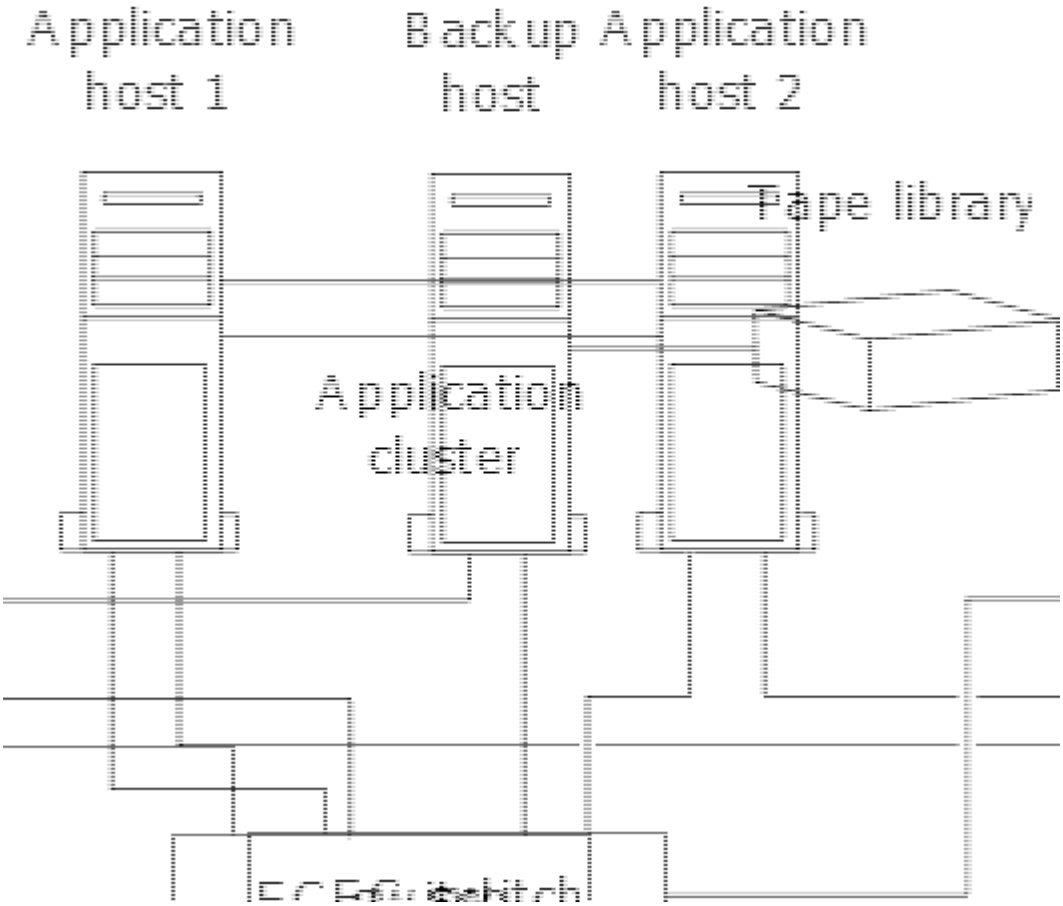
Informations associées

- "restauration snapmirror"
- "spectacle snapmirror"

Configuration recommandée pour connecter un système de sauvegarde hôte à ONTAP

Vous pouvez sauvegarder les systèmes SAN sur bande via un hôte de sauvegarde distinct afin d'éviter une dégradation des performances de l'hôte applicatif.

Il est impératif de maintenir l'séparation des données SAN et NAS à des fins de sauvegarde. La figure ci-dessous présente la configuration physique recommandée pour un système de sauvegarde hôte sur le système de stockage primaire. Vous devez configurer des volumes en tant que SAN uniquement. Les LUN peuvent être limités à un seul volume ou être répartis sur plusieurs volumes ou systèmes de stockage.



Les volumes d'un hôte peuvent être constitués d'une seule LUN mappée à partir du système de stockage ou de plusieurs LUN à l'aide d'un gestionnaire de volumes, tel que VxVM sur des systèmes HP-UX.

Utilisez un système de sauvegarde hôte pour protéger un LUN sur votre système de stockage ONTAP

Vous pouvez utiliser une LUN clonée à partir d'un snapshot comme données source pour le système de sauvegarde hôte.

Avant de commencer

Une LUN de production doit exister et être mappée sur un groupe initiateur qui inclut le WWPN ou le nom de nœud initiateur du serveur d'applications. La LUN doit également être formatée et accessible pour l'hôte

Étapes

1. Enregistrez le contenu des tampons du système de fichiers hôte sur le disque.

   Vous pouvez utiliser la commande fournie par le système d'exploitation hôte ou utiliser SnapDrive pour Windows ou SnapDrive pour UNIX. Vous pouvez également choisir de faire de cette étape une partie de votre script de prétraitement de sauvegarde SAN.

2. Créer un snapshot de la LUN de production.

   ```
   volume snapshot create -vserver <SVM_name> -volume <volume_name>
   -snapshot <snapshot> -comment <comment> -foreground false
   ```

3. Créer un clone de la LUN de production.

   ```
   volume file clone create -vserver <SMV_name> -volume <volume> -source
   -path <path> -snapshot-name <snapshot> -destination-path
   <destination_path>
   ```

4. Créez un groupe initiateur qui inclut le WWPN du serveur de sauvegarde.

   ```
   lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
   <protocol> -ostype <os_type> -initiator <initiator>
   ```

5. Mappez le clone de LUN que vous avez créé à l'étape 3 sur l'hôte de sauvegarde.

   ```
   lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
   <lun_name> -igroup <igroup>
   ```

   Vous pouvez choisir de faire de cette étape une partie du script post-traitement de votre application de sauvegarde SAN.

6. Depuis l'hôte, découvrez le nouveau LUN et rendez le système de fichiers disponible pour l'hôte.

   Vous pouvez choisir de faire de cette étape une partie du script post-traitement de votre application de sauvegarde SAN.

7. Sauvegardez les données du clone de LUN de l'hôte de sauvegarde sur bande à l'aide de votre application de sauvegarde SAN.
8. Mettre le clone de LUN hors ligne.

   ```
   lun modify -vserver <SVM_name> -path <path> -state offline
   ```

9. Supprimez le clone de LUN.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. Supprimer l'instantané.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

Référence de configuration SAN

En savoir plus sur la configuration SAN ONTAP

Un SAN (Storage Area Network) se compose d'une solution de stockage connectée à des hôtes via un protocole de transport SAN tel qu'iSCSI ou FC. Vous pouvez configurer votre SAN de sorte que votre solution de stockage se connecte à vos hôtes via un ou plusieurs commutateurs. Si vous utilisez iSCSI, vous pouvez également configurer votre SAN de sorte que votre solution de stockage se connecte directement à votre hôte sans utiliser de commutateur.

Dans un SAN, plusieurs hôtes, utilisant différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder à la solution de stockage en même temps. Vous pouvez utiliser "Mappage de LUN sélectif" et "ensembles de ports" pour limiter l'accès aux données entre les hôtes et le stockage.

Pour iSCSI, la topologie réseau entre la solution de stockage et les hôtes est appelée réseau. Pour FC, FC/NVMe et FCoE, la topologie réseau entre la solution de stockage et les hôtes est appelée structure. Pour créer une redondance, ce qui vous protège contre la perte d'accès aux données, vous devez configurer votre SAN avec des paires haute disponibilité dans une configuration multi-réseau ou multi-structure. Les configurations utilisant des nœuds uniques ou des réseaux/structures uniques ne sont pas entièrement redondants et ne sont donc pas recommandées.

Une fois votre SAN configuré, vous pouvez le faire "Provisionnez le stockage pour iSCSI ou FC", ou vous pouvez "Provisionnez le stockage pour FC/NVMe". Vous pouvez ensuite vous connecter à vos hôtes pour commencer à assurer la maintenance des données.

La prise en charge du protocole SAN varie en fonction de votre version de ONTAP, de votre plateforme et de votre configuration. Pour plus de détails sur votre configuration spécifique, reportez-vous au "Matrice d'interopérabilité NetApp".

Informations associées

- "Présentation de l'administration SAN"
- "Configuration, prise en charge et limitations de NVMe"

Configurations iSCSI

Configurez les réseaux iSCSI avec les systèmes ONTAP

Vous devez configurer votre configuration iSCSI avec des paires haute disponibilité qui se connectent directement à vos hôtes SAN iSCSI ou qui se connectent à vos hôtes via

un ou plusieurs commutateurs IP.

"Paires HA" Sont définis comme nœuds de reporting pour les chemins Active/Optimized et Active/UnOptimized qui seront utilisés par les hôtes pour accéder aux LUN. Plusieurs hôtes, utilisant différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder au stockage en même temps. Les hôtes nécessitent qu'une solution de chemins d'accès multiples prise en charge qui prend en charge ALUA soit installée et configurée. Les systèmes d'exploitation et les solutions de chemins d'accès multiples pris en charge peuvent être vérifiés sur le "Matrice d'interopérabilité NetApp".

Dans une configuration multi-réseau, deux ou plusieurs commutateurs connectent les hôtes au système de stockage. Les configurations multi-réseau sont recommandées car elles sont entièrement redondantes. Dans une configuration à réseau unique, un commutateur connecte les hôtes au système de stockage. Les configurations à un seul réseau ne sont pas entièrement redondantes.

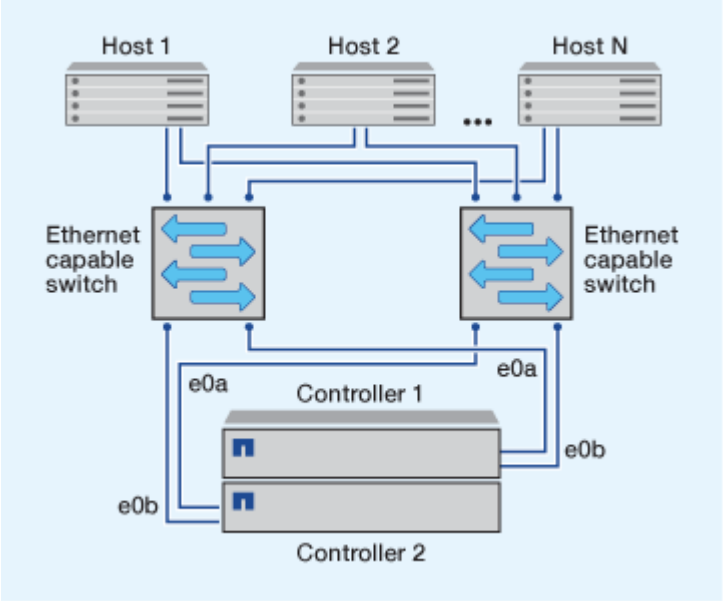
> "Configurations à un seul nœud" ne sont pas recommandées, car elles n'offrent pas la redondance nécessaire à la prise en charge de la tolérance aux pannes et de la continuité de l'activité.

Informations associées

- Découvrez comment "Mappage de LUN sélectif (SLM)" limiter les chemins utilisés pour accéder aux LUN appartenant à une paire haute disponibilité.
- Découvrez "LIF SAN".
- Découvrez le "Avantages des VLAN dans iSCSI".

Configurations iSCSI multi-réseau

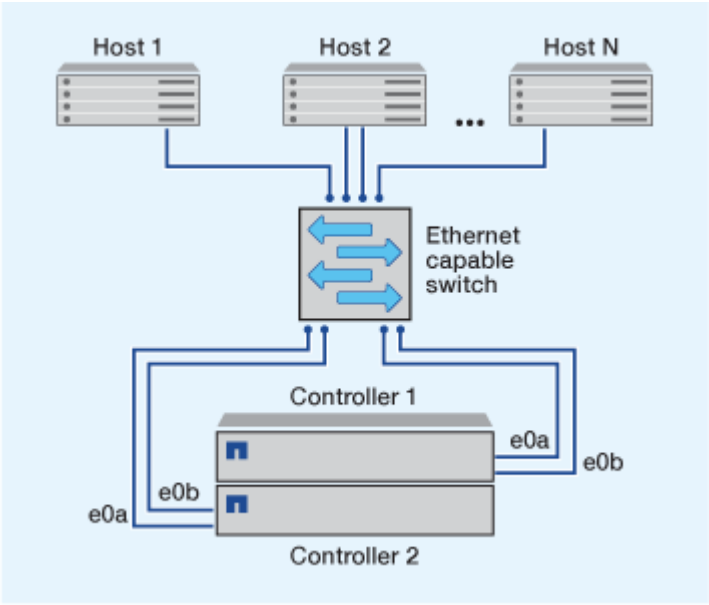
Dans les configurations de paires haute disponibilité à plusieurs réseaux, au moins deux commutateurs connectent la paire haute disponibilité à un ou plusieurs hôtes. Étant donné qu'il y a plusieurs commutateurs, cette configuration est totalement redondante.



Configurations iSCSI à réseau unique

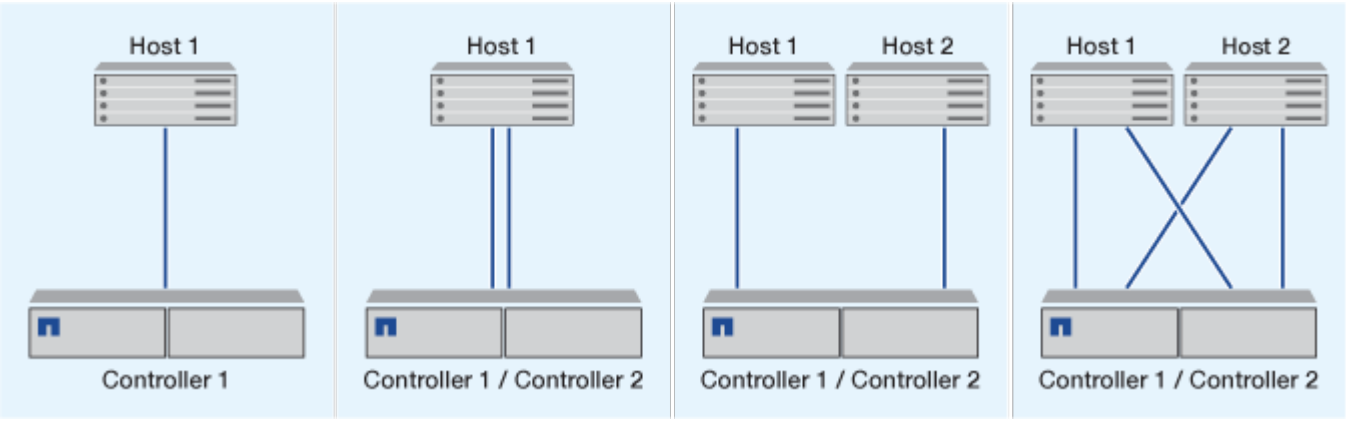
Dans les configurations de paires haute disponibilité à réseau unique, un switch connecte la paire haute disponibilité à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas

entièrement redondante.



Configuration iSCSI à connexion directe

Dans une configuration en attachement direct, un ou plusieurs hôtes sont directement connectés aux contrôleurs.



Avantages de l'utilisation de VLAN avec des systèmes ONTAP dans des configurations iSCSI

Un VLAN se compose d'un groupe de ports de commutateur regroupés dans un domaine de broadcast. Un VLAN peut se trouver sur un seul commutateur ou s'étendre sur plusieurs châssis de commutateur. Les VLAN statiques et dynamiques vous permettent d'accroître la sécurité, d'isoler les problèmes et de limiter les chemins disponibles au sein de votre infrastructure de réseau IP.

Lorsque vous implémentez des VLAN dans de grandes infrastructures de réseaux IP, vous bénéficiez des avantages suivants :

- Sécurité renforcée.

  Les VLAN vous permettent d'exploiter l'infrastructure existante tout en améliorant la sécurité, car ils limitent l'accès entre différents nœuds d'un réseau Ethernet ou d'un SAN IP.

- Amélioration de la fiabilité du réseau Ethernet et du SAN IP en isolant les problèmes.
- Réduction du temps de résolution des problèmes en limitant l'espace dédié au problème
- Réduction du nombre de chemins disponibles vers un port cible iSCSI spécifique.
- Réduction du nombre maximal de chemins utilisés par un hôte.

  Un trop grand nombre de chemins ralentit les temps de reconnexion. Si un hôte ne dispose pas d'une solution de chemins d'accès multiples, vous pouvez utiliser des VLAN pour n'autoriser qu'un seul chemin.

VLAN dynamiques

Les VLAN dynamiques sont basés sur une adresse MAC. Vous pouvez définir un VLAN en spécifiant l'adresse MAC des membres que vous souhaitez inclure.

Les VLAN dynamiques offrent une flexibilité accrue et ne nécessitent pas de mappage vers les ports physiques sur lesquels le périphérique est physiquement connecté au commutateur. Vous pouvez déplacer un câble d'un port à un autre sans reconfigurer le VLAN.

VLAN statiques

Les VLAN statiques sont basés sur des ports. Le commutateur et le port du commutateur sont utilisés pour définir le VLAN et ses membres.

Les VLAN statiques offrent une sécurité améliorée car il n'est pas possible d'enfreindre les VLAN à l'aide d'une usurpation MAC (Media Access Control). Cependant, si une personne a un accès physique au commutateur, le remplacement d'un câble et la reconfiguration de l'adresse réseau peuvent autoriser l'accès.

Dans certains environnements, il est plus facile de créer et de gérer des VLAN statiques que des VLAN dynamiques. En effet, les VLAN statiques nécessitent uniquement la spécification de l'identifiant du commutateur et du port, au lieu de l'adresse MAC 48 bits. En outre, vous pouvez étiqueter les plages de ports de commutateur avec l'identifiant VLAN.

Configurations FC

Configurez les fabrics FC ou FC-NVMe avec les systèmes ONTAP

Il est recommandé de configurer vos hôtes SAN FC et FC-NVMe à l'aide de paires haute disponibilité et d'un minimum de deux commutateurs. Cela assure la redondance aux couches de la structure et du système de stockage pour prendre en charge la tolérance aux pannes et la continuité de l'activité. Vous ne pouvez pas connecter directement des hôtes SAN FC ou FC-NVMe à des paires haute disponibilité sans utiliser de commutateur.

Les tissus en cascade, à maillage partiel, à maillage complet, à la périphérie du cœur et au directeur sont tous des méthodes standard de connexion des commutateurs FC à un tissu, et toutes sont prises en charge. L'utilisation de structures de commutateurs FC hétérogènes n'est pas prise en charge, sauf dans le cas de commutateurs lame intégrés. Des exceptions spécifiques sont répertoriées sur le "Matrice d'interopérabilité". Une structure peut comprendre un ou plusieurs commutateurs et les contrôleurs de stockage peuvent être connectés à plusieurs commutateurs.

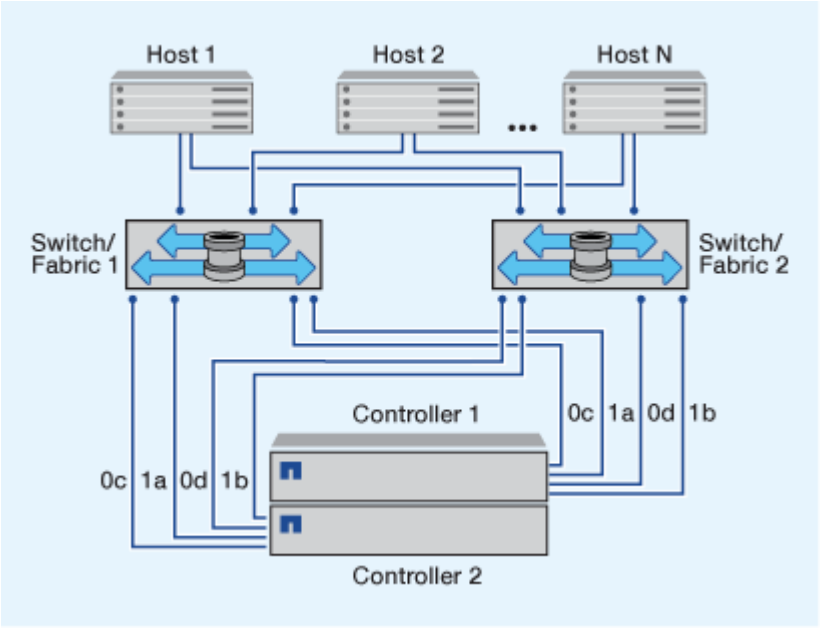
Plusieurs hôtes, qui utilisent différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder aux contrôleurs de stockage en même temps. Les hôtes nécessitent l'installation et la configuration

d'une solution de chemins d'accès multiples prise en charge. Les systèmes d'exploitation et les solutions de chemins d'accès multiples pris en charge peuvent être vérifiés à l'aide de l'outil Interoperability Matrix Tool.

Les configurations FC et FC-NVMe de Multifabric

Dans les configurations de paires haute disponibilité multistructures, il existe au moins deux commutateurs qui connectent les paires haute disponibilité à un ou plusieurs hôtes. Pour plus de simplicité, la figure suivante de paire haute disponibilité multistructure ne présente que deux fabrics, mais vous pouvez avoir au moins deux fabrics dans n'importe quelle configuration multistructure.

Les numéros de port cible FC (0C, 0d, 1a, 1b) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.

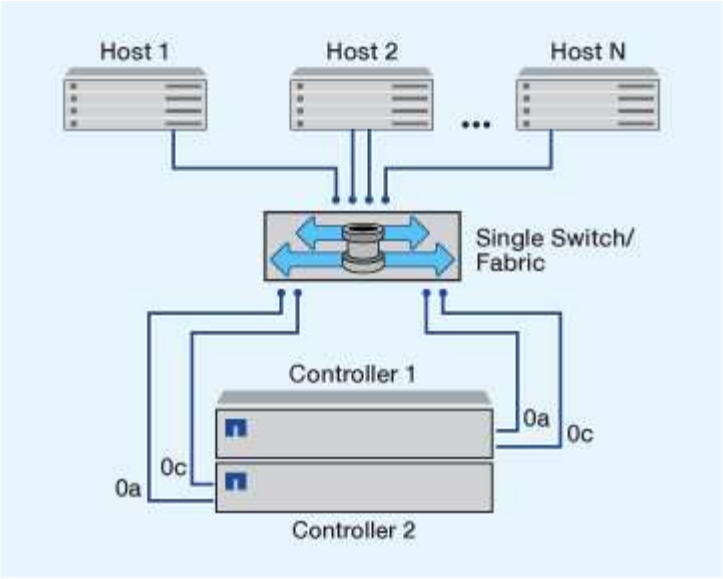


Les configurations FC et FC-NVMe à structure unique

Dans les configurations de paires haute disponibilité à structure unique, une structure relie les deux contrôleurs de la paire haute disponibilité à un ou plusieurs hôtes. Comme les hôtes et les contrôleurs sont connectés via un commutateur unique, les configurations de paires haute disponibilité à structure unique ne sont pas entièrement redondantes.

Les numéros de port FC cible (0a, 0C) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.

Toutes les plateformes qui prennent en charge les configurations FC prennent en charge les paires haute disponibilité à structure unique.



"Configurations à un seul nœud" ne sont pas recommandées, car elles n'offrent pas la redondance nécessaire à la prise en charge de la tolérance aux pannes et de la continuité de l'activité.

Informations associées

- Découvrez comment "Mappage de LUN sélectif (SLM)" limiter les chemins utilisés pour accéder aux LUN appartenant à une paire haute disponibilité.
- Découvrez "LIF SAN".

Bonnes pratiques de configuration des commutateurs FC avec les systèmes ONTAP

Pour obtenir des performances optimales, vous devez tenir compte de certaines des meilleures pratiques lors de la configuration du commutateur FC.

Un paramètre de vitesse de liaison fixe est la meilleure pratique pour les configurations de commutateurs FC, en particulier pour les structures importantes, car il offre les meilleures performances pour les reconstructions de structures et peut gagner beaucoup de temps. Bien que la négociation automatique offre la plus grande flexibilité, la configuration des commutateurs FC ne fonctionne pas toujours comme prévu, et elle ajoute du temps à la séquence globale de création de la structure.

Tous les commutateurs connectés à la structure doivent prendre en charge la virtualisation NPIV (N_Port ID Virtualization) et doivent avoir NPIV activé. ONTAP utilise NPIV pour présenter les cibles FC à une structure.

Pour plus d'informations sur les environnements pris en charge, reportez-vous au "Matrice d'interopérabilité NetApp".

Pour connaître les meilleures pratiques en matière de FC et d'iSCSI, reportez-vous à "Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"la section.

Vitesses et configuration recommandées des ports FC target pour les systèmes ONTAP

Les ports cibles FC peuvent être configurés et utilisés pour le protocole FC-NVMe de la même manière qu'ils sont configurés et utilisés pour le protocole FC. La prise en charge du protocole FC-NVMe varie en fonction de votre plateforme et de votre version de

ONTAP. Utilisez NetApp Hardware Universe pour vérifier le support.

Pour des performances optimales et une disponibilité optimale, vous devez utiliser la configuration de port cible recommandée indiquée dans le "NetApp Hardware Universe" pour votre plate-forme spécifique.

Configuration des ports FC target avec ASIC partagés

Les plates-formes suivantes ont des paires de ports avec des circuits intégrés (ASIC) partagés propres aux applications. Si vous utilisez un adaptateur d'extension avec ces plates-formes, vous devez configurer vos ports FC de sorte qu'ils n'utilisent pas le même ASIC pour la connectivité.

Contrôleur	Paires de ports avec ASIC partagé	Nombre de ports cibles : ports recommandés
• FAS8200 • AFF A300	0g+0h	1 : 0g 2 : 0g, 0h
• FAS2720 • FAS2750 • AVEC AFF A220	0c+0d 0e+0f	1 : 0c 2 : 0c, 0e 3 : 0c, 0e, 0d 4 : 0c, 0e, 0d, 0f

Vitesses prises en charge par le port FC cible

Les ports cibles FC peuvent être configurés pour s'exécuter à différentes vitesses. Tous les ports cibles utilisés par un hôte donné doivent être définis sur la même vitesse. Vous devez définir la vitesse du port cible en fonction de la vitesse du périphérique auquel il se connecte. N'utilisez pas la négociation automatique pour la vitesse de votre port. Un port défini pour la négociation automatique peut prendre plus de temps pour se reconnecter après un basculement/rétablissement ou une autre interruption.

Vous pouvez configurer les ports intégrés et les adaptateurs d'extension pour qu'ils s'exécutent à la vitesse suivante. Chaque contrôleur et port d'adaptateur d'extension peuvent être configurés individuellement pour différentes vitesses, selon les besoins.

Ports 4 Go	Ports 8 Gb	Ports 16 Gb	Ports 32 Gb
• 4 Go • 2 Go • 1 Go	• 8 Go • 4 Go • 2 Go	• 16 Go • 8 Go • 4 Go	• 32 Go • 16 Go • 8 Go

Pour obtenir la liste complète des cartes prises en charge et de leurs vitesses prises en charge, consultez le "NetApp Hardware Universe".

Configuration des ports d'adaptateur FC ONTAP

Les adaptateurs FC intégrés et certaines cartes d'adaptateur d'extension FC peuvent être configurés individuellement en tant qu'initiateurs ou ports cibles. Les autres adaptateurs d'extension FC sont configurés en usine en tant qu'initiateurs ou cibles et ne peuvent pas être modifiés. Des ports FC supplémentaires sont également disponibles via les cartes UTA2 prises en charge configurées avec les adaptateurs FC SFP+.

Les ports initiateurs peuvent être utilisés pour se connecter directement aux tiroirs disques back-end, et éventuellement à des baies de stockage étrangères. Les ports cibles peuvent être utilisés pour la connexion uniquement aux commutateurs FC.

Le nombre de ports intégrés et de ports CNA/UTA2 configurés pour FC varie en fonction du modèle du contrôleur. Les adaptateurs d'extension de cible pris en charge varient également en fonction du modèle de contrôleur. Reportez-vous à la "NetApp Hardware Universe" pour obtenir la liste complète des ports FC intégrés et des adaptateurs d'extension cible pris en charge pour votre modèle de contrôleur.

Configurer les adaptateurs FC pour le mode initiateur

Le mode initiateur permet de connecter les ports aux lecteurs de bande, aux bibliothèques de bandes ou aux systèmes de stockage tiers via l'importation de LUN étrangers (FLI).

Avant de commencer

- Les LIF présentes sur l'adaptateur doivent être supprimées de n'importe quel ensemble de ports dont elles sont membres.
- Toutes les LIF de chaque machine virtuelle de stockage (SVM) utilisant le port physique à modifier doivent être migrées ou détruites avant de changer la personnalité du port physique de la cible à l'initiateur.

> Le protocole NVMe/FC prend en charge le mode initiateur.

Étapes

1. Supprimer toutes les LIFs de l'adaptateur :

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. Mettez votre adaptateur hors ligne :

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

   Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Modifiez l'adaptateur de la cible à l'initiateur :

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.
5. Vérifier que les ports FC sont configurés dans l'état approprié pour votre configuration :

```
system hardware unified-connect show
```

6. Remettre la carte en ligne :

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

Configurer les adaptateurs FC pour le mode cible

Le mode cible est utilisé pour connecter les ports aux initiateurs FC.

Les mêmes étapes sont utilisées pour configurer les adaptateurs FC pour le protocole FC et le protocole FC-NVMe. Cependant, seuls certains adaptateurs FC prennent en charge la connectivité FC-NVMe. Consultez la "NetApp Hardware Universe" pour obtenir la liste des adaptateurs qui prennent en charge le protocole FC-NVMe.

Étapes

1. Mettez l'adaptateur hors ligne :

   ```
   node run -node _node_name_ storage disable adapter _adapter_name_
   ```

   Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

2. Modifiez l'adaptateur de l'initiateur sur la cible :

   ```
   system node hardware unified-connect modify -t target -node _node_name_
   adapter _adapter_name_
   ```

3. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.
4. Vérifiez que la configuration du port cible est correcte :

   ```
   network fcp adapter show -node _node_name_
   ```

5. Mettez votre adaptateur en ligne :

   ```
   network fcp adapter modify -node _node_name_ -adapter _adapter_port_
   -state up
   ```

Configuration de la vitesse de l'adaptateur FC

Vous devez configurer la vitesse du port cible de votre carte pour qu'elle corresponde à la vitesse du périphérique auquel elle se connecte, au lieu d'utiliser la négociation automatique. Un port défini pour la négociation automatique peut prendre plus de temps pour se reconnecter après un basculement/rétablissement ou une autre interruption.

Description de la tâche

Cette tâche englobant tous les SVM (Storage Virtual machine) et toutes les LIFs d'un cluster, vous devez utiliser le `-home-port` et `-home-lif` paramètres pour limiter la portée de cette opération. Si vous n'utilisez

pas ces paramètres, l'opération s'applique à toutes les LIFs du cluster, ce qui peut ne pas être souhaitable.

Avant de commencer

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

Étapes

1. Mettre hors ligne toutes les LIFs sur cet adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. Mettez l'adaptateur hors ligne :

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

   Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Déterminez la vitesse maximale de l'adaptateur de port :

```
fcp adapter show -instance
```

   Vous ne pouvez pas modifier la vitesse de l'adaptateur au-delà de la vitesse maximale.

4. Modifier la vitesse de l'adaptateur :

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Mettez la carte en ligne :

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Mettre en ligne toutes les LIFs sur l'adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

Commandes ONTAP pour la gestion des adaptateurs FC

Vous pouvez utiliser des commandes FC pour gérer les adaptateurs cibles FC, les adaptateurs initiateurs FC et les adaptateurs FC intégrés à votre contrôleur de stockage. Les mêmes commandes sont utilisées pour gérer les adaptateurs FC pour le protocole

FC et le protocole FC-NVMe.

Les commandes de l'adaptateur initiateur FC fonctionnent uniquement au niveau du nœud. Vous devez utiliser le `run -node node_name` Commande avant de pouvoir utiliser les commandes de l'adaptateur FC initiator.

Commandes de gestion des adaptateurs cibles FC

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche les informations relatives à l'adaptateur FC sur un nœud	`network fcp adapter show`
Modifiez les paramètres de l'adaptateur cible FC	`network fcp adapter modify`
Affiche les informations de trafic du protocole FC	`run -node node_name sysstat -f`
Afficher la durée d'exécution du protocole FC	`run -node node_name uptime`
Affiche la configuration et l'état de la carte	`run -node node_name sysconfig -v adapter`
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	`run -node node_name sysconfig -ac`
Affichez une page man pour une commande	`man command_name`

Commandes de gestion des adaptateurs initiateurs FC

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche les informations relatives à la totalité des initiateurs et de leurs adaptateurs dans un nœud	`run -node node_name storage show adapter`
Affiche la configuration et l'état de la carte	`run -node node_name sysconfig -v adapter`
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	`run -node node_name sysconfig -ac`

Commandes de gestion des adaptateurs FC intégrés

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche l'état des ports FC intégrés	`system node hardware unified-connect show`

Informations associées

- "adaptateur réseau fcp"

Évitez toute perte de connectivité avec un système ONTAP à l'aide d'un adaptateur X1133A-R6

Vous pouvez éviter la perte de connectivité lors d'une défaillance de port en configurant votre système avec des chemins redondants vers des HBA X1133A-R6 distincts.

La carte HBA X1133A-R6 est un adaptateur FC 16 Gbit à 4 ports composé de deux paires à 2 ports. L'adaptateur X1133A-R6 peut être configuré en mode cible ou initiateur. Chaque paire de 2 ports est prise en charge par un seul ASIC (par exemple, les ports 1 et 2 sur ASIC 1 et les ports 3 et 4 sur ASIC 2). Les deux ports d'un ASIC unique doivent être configurés pour fonctionner dans le même mode, soit en mode cible, soit en mode initiateur. En cas d'erreur sur l'ASIC prenant en charge une paire, les deux ports de la paire sont mis hors ligne.

Pour éviter ce risque de perte de connectivité, vous devez configurer votre système avec des chemins redondants vers des HBA X1133A-R6 distincts, ou avec des chemins redondants vers des ports pris en charge par différents ASIC sur le HBA.

Configurations FCoE

Configurez les structures FCoE avec les systèmes ONTAP

FCoE peut être configuré de différentes manières avec les commutateurs FCoE. Les configurations à connexion directe ne sont pas prises en charge par la FCoE.

Toutes les configurations FCoE sont à double structure, entièrement redondantes et requièrent un logiciel de chemins d'accès multiples côté hôte. Dans toutes les configurations FCoE, vous pouvez avoir plusieurs commutateurs FCoE et FC dans le chemin entre l'initiateur et la cible, dans la limite maximale du nombre de sauts. Pour connecter les commutateurs les uns aux autres, les commutateurs doivent exécuter une version de firmware qui prend en charge les liens ISL Ethernet. Dans toutes les configurations FCoE, chaque hôte peut être configuré avec un système d'exploitation différent.

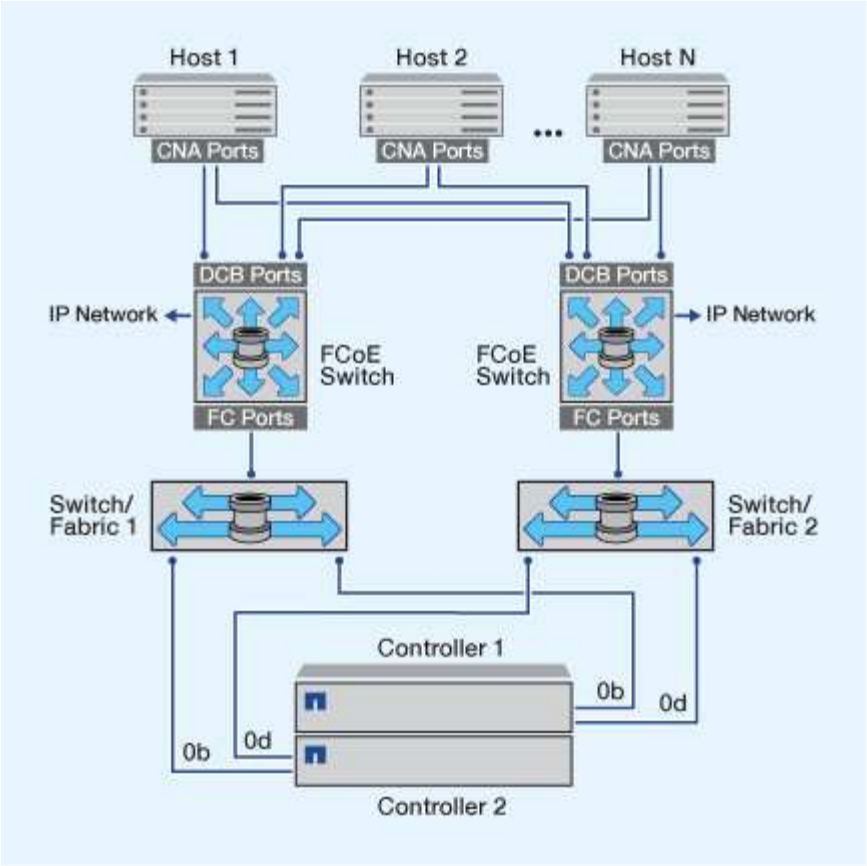
Les configurations FCoE requièrent des commutateurs Ethernet qui prennent explicitement en charge les fonctionnalités FCoE. Les configurations FCoE sont validées par le biais du même processus d'interopérabilité et d'assurance qualité que les commutateurs FC. Les configurations prises en charge sont répertoriées dans la matrice d'interopérabilité. Certains paramètres inclus dans ces configurations prises en charge sont le modèle de commutateur, le nombre de commutateurs pouvant être déployés dans une structure unique et la version de micrologiciel du commutateur prise en charge.

Les numéros de ports des adaptateurs d'extension FC target de l'illustration sont à titre d'exemples. Les numéros réels des ports peuvent varier en fonction des connecteurs d'extension dans lesquels les adaptateurs d'extension de la cible FCoE sont installés.

Initiateur FCoE sur la cible FC

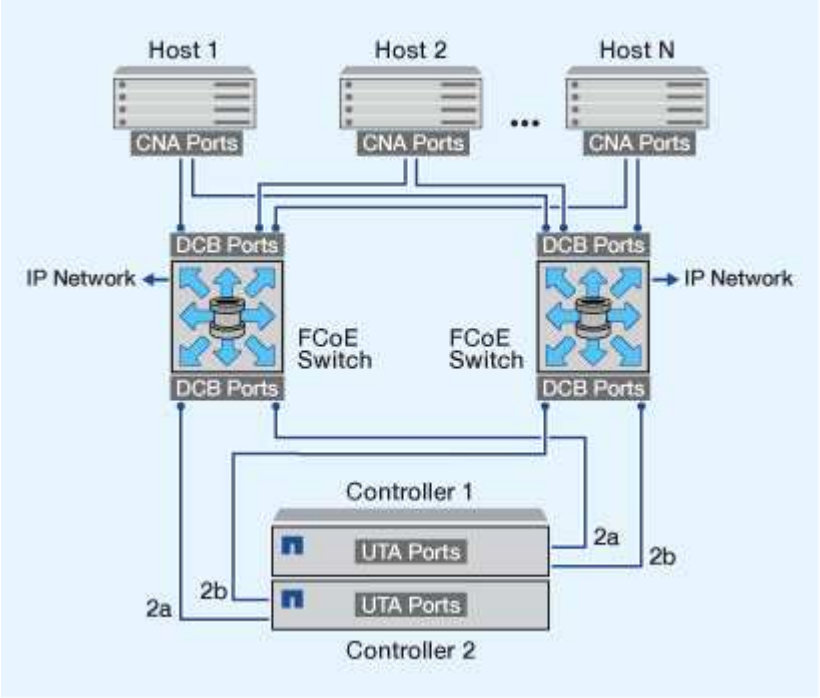
En utilisant les initiateurs FCoE (CNA), vous pouvez connecter des hôtes aux deux contrôleurs d'une paire haute disponibilité via des commutateurs FCoE vers les ports cible FC. Le commutateur FCoE doit également posséder des ports FC. L'initiateur FCoE hôte se connecte toujours au commutateur FCoE. Le commutateur FCoE peut se connecter directement à la cible FC ou se connecter à la cible FC via des commutateurs FC.

L'illustration suivante montre les CNA hôtes connectés à un commutateur FCoE, puis à un commutateur FC avant de se connecter à la paire haute disponibilité :



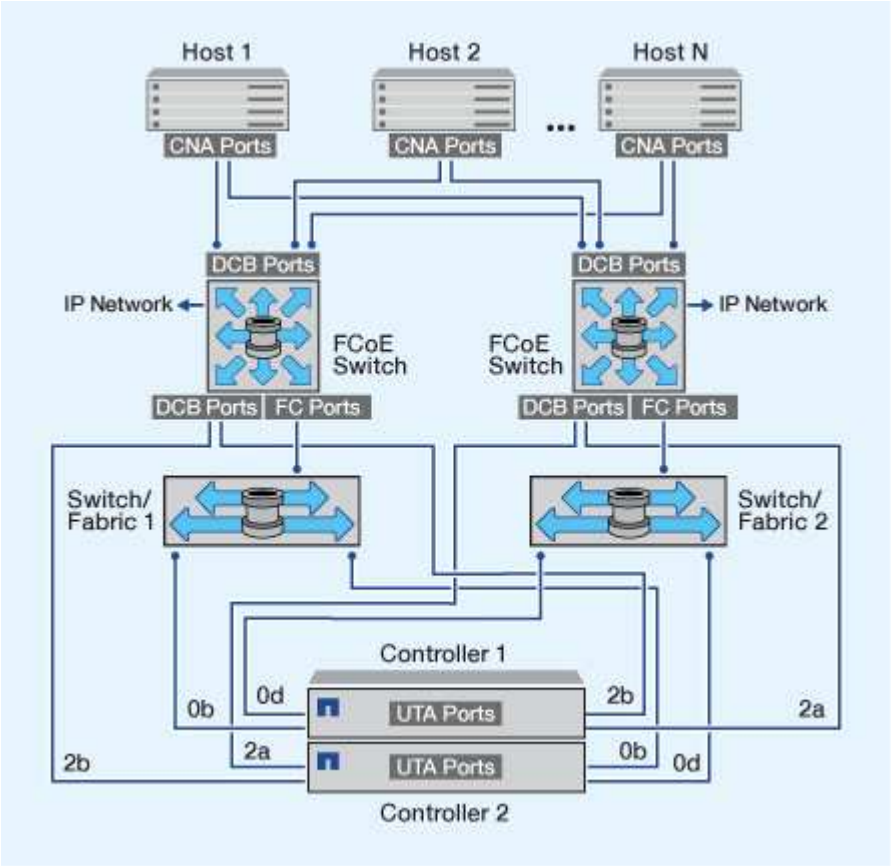
Initiateur FCoE vers la cible FCoE

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE (également appelés UTAS ou UTA2) à l'aide des commutateurs FCoE.



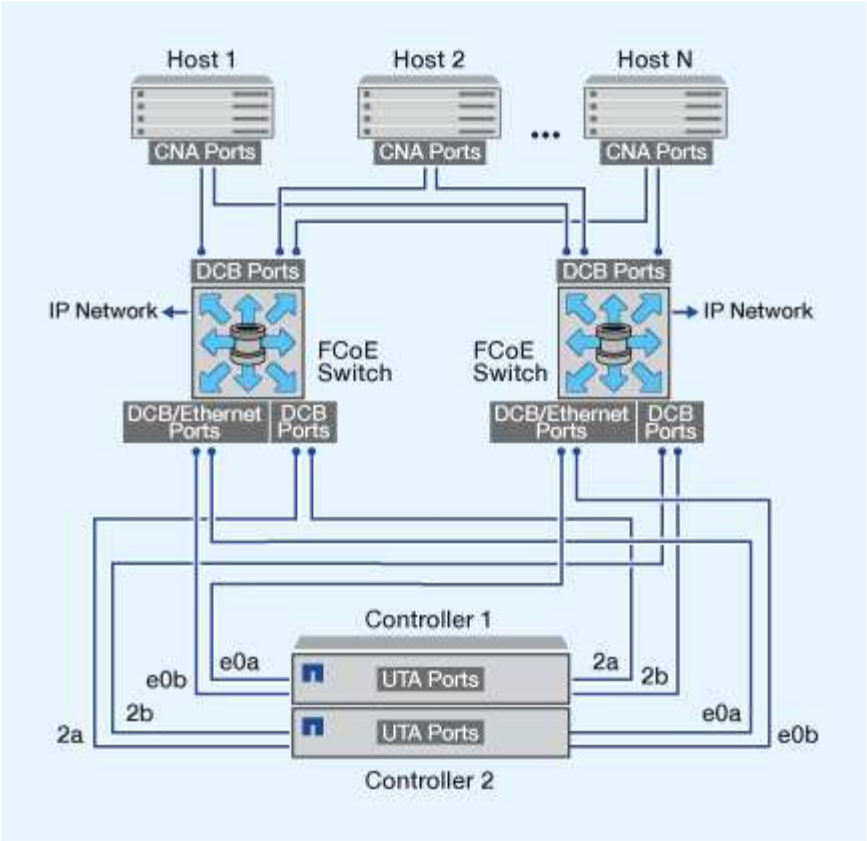
Initiateur FCoE sur les cibles FCoE et FC

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE et FC (également appelés UTA ou UTA2) à l'aide des commutateurs FCoE.



FCoE combiné avec les protocoles de stockage IP

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE (également appelés UTAS ou UTA2) à l'aide des commutateurs FCoE. Les ports FCoE ne peuvent pas utiliser l'agrégation de liens traditionnelle vers un commutateur unique. Les commutateurs Cisco prennent en charge un type spécial d'agrégation de liens (Virtual Port Channel) qui prend en charge le protocole FCoE. Un canal de port virtuel rassemble des liaisons individuelles vers deux commutateurs. Vous pouvez également utiliser les canaux de port virtuel pour d'autres trafics Ethernet. Les ports utilisés pour le trafic autre que FCoE, notamment les protocoles NFS, SMB, iSCSI et tout autre trafic Ethernet, peuvent utiliser des ports Ethernet classiques sur les switchs FCoE.



ONTAP prend en charge les combinaisons de ports cible et d'initiateur FCoE

Certaines combinaisons d'initiateurs et de cibles FCoE et FC classiques sont prises en charge.

Initiateurs FCoE

Vous pouvez utiliser des initiateurs FCoE dans des ordinateurs hôtes avec des cibles FCoE et FC traditionnelles dans des contrôleurs de stockage. L'initiateur FCoE de l'hôte doit se connecter à un commutateur DCB (pontage du centre de données) FCoE ; la connexion directe à une cible n'est pas prise en charge.

Le tableau suivant répertorie les combinaisons prises en charge :

Initiateur	Cible	Pris en charge ?
FC	FC	Oui.
FC	FCoE	Oui.
FCoE	FC	Oui.
FCoE	FCoE	Oui.

Cibles de la FCoE

Vous pouvez combiner les ports cibles FCoE avec des ports FC 4 Go, 8 Go ou 16 Go sur le contrôleur de stockage, que les ports FC soient des adaptateurs cibles supplémentaires ou des ports intégrés. Vous pouvez avoir des adaptateurs cibles FCoE et FC dans le même contrôleur de stockage.

> Les règles relatives à l'association des ports FC intégrés et d'extension sont toujours applicables.

Segmentation FC et FCoE

En savoir plus sur le zoning FC et FCoE avec les systèmes ONTAP

Une zone FC, FC-NVMe ou FCoE est un regroupement logique d'un ou de plusieurs ports au sein d'une structure. Pour que les périphériques puissent se voir, se connecter, créer des sessions entre eux et communiquer, les deux ports doivent être membres de la même zone.

Le zonage renforce la sécurité en limitant l'accès et la connectivité aux points de terminaison qui partagent une zone commune. Les ports qui ne se trouvent pas dans la même zone ne peuvent pas communiquer entre eux. Cela réduit ou élimine la *diaphonie* entre les HBA initiateurs. Si des problèmes de connectivité se produisent, la segmentation contribue à isoler les problèmes vers un ensemble spécifique de ports, ce qui réduit le temps de résolution.

Le zoning réduit le nombre de chemins disponibles vers un port particulier et le nombre de chemins entre un hôte et le système de stockage. Par exemple, certaines solutions de chemins d'accès multiples du système d'exploitation hôte ont une limite sur le nombre de chemins qu'elles peuvent gérer. La segmentation peut réduire le nombre de chemins visibles pour l'hôte de sorte que les chemins vers l'hôte ne dépassent pas le maximum autorisé par le système d'exploitation hôte.

Segmentation basée sur le World Wide Name

La segmentation basée sur le World Wide Name (WWN) spécifie le WWN des membres à inclure dans la zone. Bien que la segmentation WWNN (World Wide Node Name) soit possible avec certains fournisseurs de commutateurs, lors du zoning dans ONTAP, vous devez utiliser la segmentation WWPN (World Wide Port Name).

La segmentation WWPN est nécessaire pour définir correctement un port spécifique et utiliser NPIV efficacement. Les commutateurs FC doivent être zonés en utilisant les WWPN des interfaces logiques (LIF) de la cible, et non les WWPN des ports physiques du nœud. Les WWPN des ports physiques commencent par « 50 » et les WWPN des LIF commencent par « 20 ».

La segmentation WWPN apporte la flexibilité, car l'accès n'est pas déterminé par l'emplacement de connexion physique du dispositif à la structure. Vous pouvez déplacer un câble d'un port à un autre sans reconfigurer les zones.

Configurations de zoning FC et FCoE recommandées pour les systèmes ONTAP

Vous devez créer une configuration de zoning si votre hôte n'a pas de solution de chemins d'accès multiples installée, si quatre hôtes ou plus sont connectés à votre SAN ou si le mappage de LUN sélectif n'est pas implémenté sur les nœuds de votre cluster.

Dans la configuration de zoning FC et FCoE recommandée, chaque zone inclut un port initiateur et une ou

plusieurs LIFs cible. Cette configuration permet à chaque initiateur hôte d'accéder à n'importe quel nœud, tout en empêchant les hôtes qui accèdent au même nœud de voir les ports des autres hôtes

Ajoutez toutes les LIFs de la machine virtuelle de stockage (SVM) à la zone avec l'initiateur hôte. Cela vous permet de déplacer des volumes ou des LUN sans modifier vos zones existantes ni créer de nouvelles zones.

Configurations de zoning Dual fabric

Les configurations de segmentation à structure double sont recommandées, car elles fournissent une protection contre la perte de données due à la défaillance d'un seul composant. Dans une configuration à structure double, chaque initiateur hôte est connecté à chaque nœud du cluster à l'aide de différents commutateurs. Si un commutateur devient indisponible, l'accès aux données est maintenu par l'autre commutateur. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples.

Dans la figure suivante, l'hôte a deux initiateurs et exécute un logiciel de chemins d'accès multiples. Il y a deux zones. "Mappage de LUN sélectif (SLM)" est configuré de sorte que tous les nœuds soient considérés comme des nœuds de reporting.

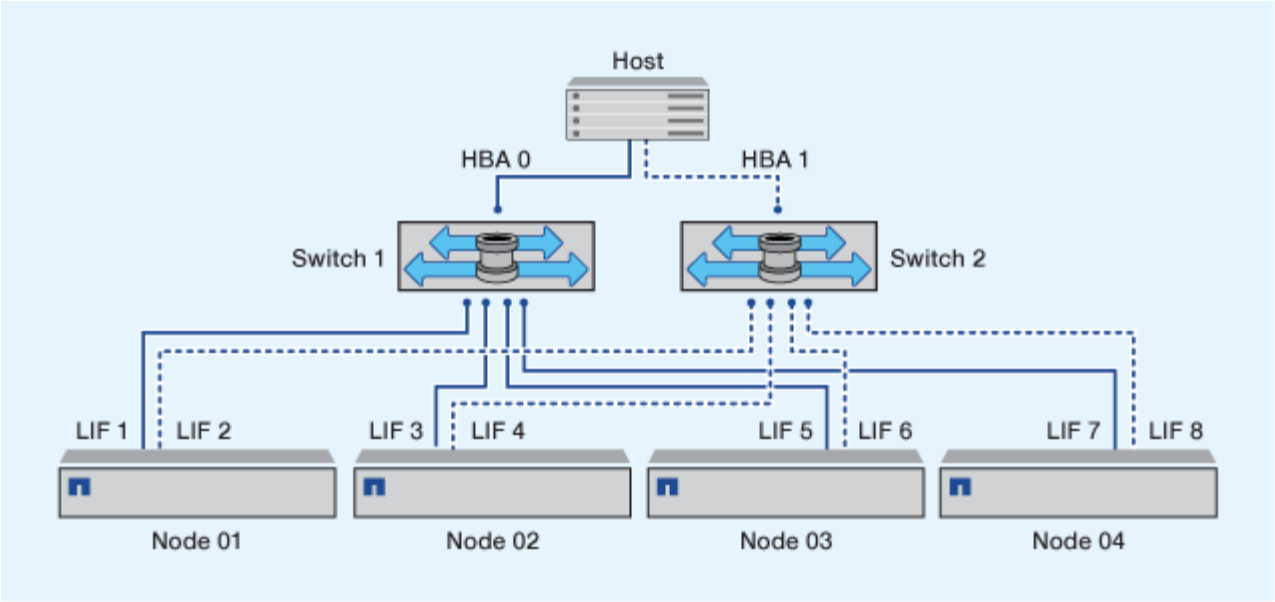
> la convention de nom utilisée dans cette figure ne constitue qu'une recommandation d'une convention de nom possible que vous pouvez utiliser pour votre solution ONTAP.

- Zone 1 : HBA 0, LIF_1, LIF_3, LIF_5 et LIF_7
- Zone 2 : HBA 1, LIF_2, LIF_4, LIF_6 et LIF_8

Chaque initiateur hôte est zoné via un autre commutateur. La zone 1 est accessible via le commutateur 1. La zone 2 est accessible via le commutateur 2.

Chaque hôte peut accéder à une LIF sur chaque nœud. Cela permet à l'hôte d'accéder toujours à ses LUN en cas de panne d'un nœud. Les SVM ont accès à toutes les LIF iSCSI et FC sur chaque nœud du cluster en fonction de la configuration des nœuds de reporting SLM. Vous pouvez utiliser la segmentation de switch SLM, portsets ou FC pour réduire le nombre de chemins d'un SVM à l'hôte et le nombre de chemins d'un SVM vers une LUN.

Si la configuration inclut plus de nœuds, les LIFs pour les nœuds supplémentaires sont incluses dans ces zones.



Le système d'exploitation hôte et le logiciel de chemins d'accès multiples doivent prendre en charge le nombre de chemins d'accès utilisés pour accéder aux LUN sur les nœuds.

Segmentation à structure unique

Dans une configuration à structure unique, vous connectez chaque initiateur hôte à chaque nœud de stockage via un commutateur unique. Les configurations de segmentation à structure unique ne sont pas recommandées, car elles n'offrent pas de protection contre la perte de données due à la défaillance d'un seul composant. Si vous choisissez de configurer la segmentation à structure unique, chaque hôte doit avoir deux initiateurs pour les chemins d'accès multiples pour fournir la résilience dans la solution. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples.

Chaque initiateur hôte doit disposer d'au moins une LIF à partir de chaque nœud auquel l'initiateur peut accéder. Le zoning doit permettre à au moins un chemin entre l'initiateur hôte et la paire haute disponibilité de nœuds dans le cluster pour fournir un chemin d'accès à la connectivité LUN. Cela signifie que chaque initiateur sur l'hôte peut ne disposer que d'une seule LIF cible par nœud dans sa configuration de zone. Si des chemins d'accès multiples sont nécessaires vers le même nœud ou vers plusieurs nœuds du cluster, chaque nœud aura plusieurs LIF par nœud dans sa configuration de zone. Cela permet à l'hôte d'accéder toujours à ses LUN en cas de défaillance d'un nœud ou si un volume contenant la LUN est déplacé vers un autre nœud. Il est également nécessaire de définir correctement les nœuds de reporting.

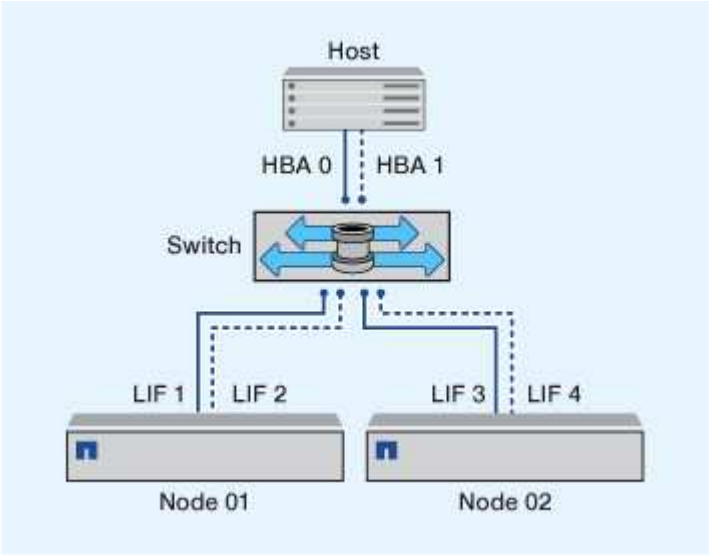
Si vous utilisez des commutateurs Cisco FC et FCoE, une seule zone de structure ne doit pas contenir plus d'une LIF cible pour le même port physique. Si plusieurs LIF présentes sur le même port se trouvent dans la même zone, les ports LIF peuvent ne pas effectuer de restauration suite à une perte de connexion.

Dans la figure suivante, l'hôte a deux initiateurs et exécute un logiciel de chemins d'accès multiples. Il y a deux zones :

la convention de nom utilisée dans cette figure ne constitue qu'une recommandation d'une convention de nom possible que vous pouvez utiliser pour votre solution ONTAP.

- Zone 1 : HBA 0, LIF_1 et LIF_3
- Zone 2 : HBA 1, LIF_2 et LIF_4

Si la configuration inclut plus de nœuds, les LIFs des nœuds supplémentaires sont incluses dans ces zones.s.



Dans cet exemple, vous pouvez aussi avoir les quatre LIF dans chaque zone. Dans ce cas, les zones seraient les suivantes :

- Zone 1 : HBA 0, LIF_1, LIF_2, LIF_3 et LIF_4
- Zone 2 : HBA 1, LIF_1, LIF_2, LIF_3 et LIF_4

> Le système d'exploitation hôte et le logiciel de chemins d'accès multiples doivent prendre en charge le nombre de chemins pris en charge qui sont utilisés pour accéder aux LUN sur les nœuds. Pour déterminer le nombre de chemins utilisés pour accéder aux LUN sur les nœuds, reportez-vous à la section limites de configuration SAN.

Restrictions de segmentation pour les commutateurs Cisco FC et FCoE

Lors de l'utilisation de commutateurs Cisco FC et FCoE, certaines restrictions s'appliquent à l'utilisation de ports physiques et d'interfaces logiques (LIF) dans les zones.

Ports physiques

- Les protocoles FC-NVMe et FC peuvent partager le même port physique de 32 Go
- Les protocoles FC-NVMe et FCoE ne peuvent pas partager le même port physique
- FC et FCoE peuvent partager le même port physique, mais la LIF de leur protocole doit se trouver dans des zones séparées.

Interfaces logiques (LIFS)

- Une zone peut contenir une LIF de chaque port cible du cluster.

  Vérifiez la configuration SLM afin de ne pas dépasser le nombre maximal de chemins autorisés pour l'hôte.

- Chaque LIF sur un port donné doit se trouver dans une zone distincte des autres LIFs sur ce port
- Les LIF présentes sur différents ports physiques peuvent se trouver dans la même zone.

Configuration requise pour les hôtes SAN connectés à des systèmes ONTAP et non NetApp

Les configurations SAN partagées sont des hôtes connectés à la fois aux systèmes de

stockage ONTAP et aux systèmes de stockage d'autres fournisseurs. L'accès aux systèmes de stockage ONTAP et aux systèmes de stockage d'autres fournisseurs à partir d'un hôte unique est pris en charge, dans la mesure où plusieurs conditions sont respectées.

Pour tous les systèmes d'exploitation hôtes, il est recommandé d'utiliser des adaptateurs distincts pour la connexion aux systèmes de stockage de chaque fournisseur. L'utilisation de cartes séparées réduit les risques de conflits entre les pilotes et les paramètres. Pour les connexions à un système de stockage ONTAP, le modèle d'adaptateur, le BIOS, le firmware et le pilote doivent être répertoriés comme pris en charge dans l'outil de matrice d'interopérabilité NetApp.

Vous devez définir les valeurs de temporisation requises ou recommandées et d'autres paramètres de stockage pour l'hôte. Vous devez toujours installer le logiciel NetApp ou appliquer les paramètres NetApp en dernier.

- Pour AIX, vous devez appliquer les valeurs de la version AIX Host Utilities répertoriée dans l'outil Interoperability Matrix Tool pour votre configuration.
- Pour ESX, vous devez appliquer les paramètres de l'hôte à l'aide de Virtual Storage Console pour VMware vSphere.
- Pour HP-UX, vous devez utiliser les paramètres de stockage par défaut HP-UX.
- Pour Linux, vous devez appliquer les valeurs de la version Linux Host Utilities répertoriée dans la matrice d'interopérabilité pour votre configuration.
- Pour Solaris, vous devez appliquer les valeurs de la version Solaris Host Utilities répertoriée dans la matrice d'interopérabilité pour votre configuration.
- Pour Windows, vous devez installer la version des utilitaires d'hôtes Windows répertoriée dans la matrice d'interopérabilité pour votre configuration.

Informations associées

"Matrice d'interopérabilité NetApp"

Configurations SAN dans un environnement MetroCluster

Configurations SAN prises en charge dans un environnement ONTAP MetroCluster

Vous devez tenir compte de certaines considérations relatives à l'utilisation des configurations SAN dans un environnement MetroCluster.

- Les configurations MetroCluster ne prennent pas en charge les configurations VSAN « routées » de la structure FC front-end.
- À partir de ONTAP 9.15.1, les configurations IP MetroCluster à quatre nœuds sont prises en charge par le protocole NVMe/TCP.
- Depuis la version ONTAP 9.12.1, les configurations IP MetroCluster à quatre nœuds sont prises en charge sur NVMe/FC. Les configurations MetroCluster ne sont pas prises en charge pour les réseaux NVMe frontaux avant ONTAP 9.12.1.
- D'autres protocoles SAN, tels que iSCSI, FC et FCoE, sont pris en charge dans les configurations MetroCluster.
- Lors de l'utilisation de configurations client SAN, vous devez vérifier si des considérations spéciales sont incluses dans les configurations MetroCluster dans les notes fournies dans le "Matrice d'interopérabilité NetApp" (IMT).

- Les systèmes d'exploitation et les applications doivent offrir une résilience d'E/S de 120 secondes pour prendre en charge le basculement automatique non planifié et le basculement manuel d'utilisation (Tiebreaker) MetroCluster.
- Les configurations MetroCluster utilisent les mêmes WWN et WWPN des deux côtés de la structure FC frontale.

Informations associées

- "Tout savoir sur la protection des données et la reprise après incident MetroCluster"
- "Article de la base de connaissances : que sont les considérations relatives à la prise en charge des hôtes AIX dans une configuration MetroCluster ?"
- "Article de la base de connaissances : considérations relatives au support des hôtes Solaris dans une configuration MetroCluster"

Évitez le chevauchement des ports lors du basculement et du rétablissement ONTAP MetroCluster

Dans un environnement SAN, vous pouvez configurer les commutateurs frontaux afin d'éviter tout chevauchement lorsque l'ancien port passe hors ligne et que le nouveau port est connecté.

Lors du basculement, le port FC du site survivant peut se connecter à la structure avant que la structure n'ait détecté que le port FC du site de reprise sur incident est hors ligne et que ce port a été supprimé du nom et des services d'annuaire.

Si le port FC de l'incident n'est pas encore supprimé, la tentative de connexion à la structure du port FC du site survivant peut être rejetée à cause d'un WWPN dupliqué. Ce comportement des commutateurs FC peut être modifié afin de respecter la connexion du périphérique précédent et non l'ancienne. Vous devez vérifier les effets de ce comportement sur d'autres périphériques de structure. Contactez le fournisseur du commutateur pour plus d'informations.

Choisissez la procédure correcte selon votre type de commutateur.

Exemple 9. Étapes

Commutateur Cisco

1. Connectez-vous au commutateur et connectez-vous.
2. Passer en mode configuration :

```
switch# config t
switch(config)#
```

3. Remplacez la première entrée de périphérique dans la base de données du serveur de noms par le nouveau périphérique :

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Dans les commutateurs exécutant NX-OS 8.x, vérifiez que le délai de mise en veille flogi est défini sur zéro :

   a. Afficher le délai de mise au repos :

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Si la sortie de l'étape précédente n'indique pas que le délai est égal à zéro, définissez-le sur zéro :

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Commutateur Brocade

1. Connectez-vous au commutateur et connectez-vous.
2. Entrez le `switchDisable` commande.
3. Entrez le `configure` et appuyez sur `y` à l'invite.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Choisir le paramètre 1 :

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Répondez aux autres invites ou appuyez sur **Ctrl + D**.
6. Entrez le `switchEnable` commande.

Informations associées

"Effectuer un basculement pour les tests ou la maintenance"

Prise en charge de ONTAP pour les chemins d'accès multiples d'hôtes SAN

ONTAP utilise le logiciel ALUA (Asymmetric Logical Unit Access) pour les chemins d'accès multiples avec les hôtes FC et iSCSI.

Depuis la version ONTAP 9.5, le basculement/rétablissement de paire haute disponibilité multivoie est pris en charge pour les hôtes NVMe qui utilisent ANA (Asynchronous Namespace Access). Dans ONTAP 9.4, NVMe ne prend en charge qu'un seul chemin de l'hôte vers la cible. L'hôte d'application doit donc gérer le basculement de chemin vers son partenaire haute disponibilité.

Le logiciel de chemins d'accès multiples est requis sur votre hôte SAN si celui-ci peut accéder à un namespace de LUN ou NVMe via plusieurs chemins. Elle présente un seul disque au système d'exploitation pour tous les chemins d'accès à un namespace de LUN ou NVMe. Sans cela, le système d'exploitation pourrait traiter chaque chemin en tant que disque distinct, ce qui aurait pour effet de corrompre les données.

Votre solution est considérée comme ayant plusieurs chemins si vous avez l'un des suivants :

- Un port initiateur unique sur l'hôte reliant plusieurs LIF SAN au sein du SVM
- Plusieurs ports initiateurs se connectant à une seule LIF SAN dans le SVM
- Plusieurs ports initiateurs qui se fixent sur plusieurs LIF SAN au sein du SVM

Un logiciel de chemins d'accès multiples, également appelé logiciel MPIO (multivoies I/O), est recommandé dans les configurations haute disponibilité. Outre le mappage de LUN sélectif, il est également recommandé d'utiliser une segmentation de commutateur FC ou des ensembles de ports pour limiter les chemins utilisés pour accéder aux LUN.

Pour plus d'informations sur les configurations d'hôte spécifiques prenant en charge ALUA ou ANA, reportez-vous au "Matrice d'interopérabilité NetApp" et "Configuration de l'hôte SAN ONTAP" pour votre système d'exploitation hôte.

Nombre recommandé de chemins entre l'hôte et les nœuds dans le cluster

Vous ne devez pas dépasser huit chemins entre l'hôte et chaque nœud du cluster. De plus, vous ne devez pas dépasser le nombre total de chemins d'accès pris en charge pour le système d'exploitation hôte et les chemins d'accès multiples utilisés sur l'hôte.

Vous devez disposer d'au moins deux chemins par LUN en vous connectant à chaque nœud de reporting via "Mappage de LUN sélectif (SLM)"leur utilisation par la machine virtuelle de stockage (SVM) dans votre cluster.

Cela élimine les points de défaillance uniques et permet au système de résister aux défaillances des composants.

Si votre cluster contient quatre nœuds ou plus, ou plus de quatre ports cibles utilisés par les SVM sur l'un de vos nœuds, Vous pouvez utiliser les méthodes suivantes pour limiter le nombre de chemins pouvant être utilisés pour accéder aux LUN sur vos nœuds. De cette manière, vous ne devez pas dépasser le maximum recommandé de huit chemins.

- SLM

  SLM réduit le nombre de chemins de l'hôte vers le LUN vers uniquement les chemins sur le nœud possédant le LUN et le partenaire HA du nœud propriétaire. SLM est activé par défaut.

- "Ensembles de ports pour iSCSI"
- Mappages de FC igroup depuis votre hôte
- Segmentation des commutateurs FC

Limites de configuration

Déterminer le nombre maximal de nœuds et d'hôtes SAN pris en charge par cluster ONTAP

Le nombre de nœuds pris en charge par cluster varie en fonction de votre version de ONTAP, de vos modèles de contrôleur et du protocole de vos nœuds de cluster. Le nombre maximal d'hôtes SAN pouvant être connectés à un cluster dépend également de votre configuration spécifique.

Déterminez le nombre maximal de nœuds pris en charge par cluster

Si un nœud du cluster est configuré pour les protocoles FC, FC-NVMe, FCoE ou iSCSI, ce cluster est limité aux limites du nœud SAN. Les limites de nœuds basées sur les contrôleurs de votre cluster sont répertoriées dans le *Hardware Universe*.

Étapes

1. Accédez à "NetApp Hardware Universe".
2. Dans le coin supérieur gauche, à côté de **Home**, sélectionnez **Platforms**, puis sélectionnez le type de plate-forme.
3. Sélectionnez votre version de ONTAP.

   Une nouvelle colonne s'affiche pour vous permettre de choisir vos plates-formes.

4. Sélectionnez les plates-formes utilisées dans votre solution.
5. Sous **Choisissez vos spécifications**, désélectionnez **Sélectionner tout**.
6. Sélectionnez **nombre max. De nœuds par cluster (NAS/SAN)**.
7. Cliquez sur **Afficher les résultats**.

Résultats

Le nombre maximal de nœuds par cluster pour les plateformes sélectionnées s'affiche.

Déterminez si votre cluster peut prendre en charge davantage d'hôtes FC

Pour les configurations FC et FC-NVMe, vous devez utiliser le nombre de nases cibles (ITN) dans votre système pour déterminer si vous pouvez ajouter d'autres hôtes à votre cluster.

Un ITN représente un chemin entre l'initiateur de l'hôte et la cible du système de stockage. Le nombre maximum de N ITN par nœud dans les configurations FC et FC-NVMe est de 2,048. Si vous êtes inférieur au nombre maximum d'ITN, vous pouvez continuer à ajouter des hôtes à votre cluster.

Pour déterminer le nombre d'ITN utilisés dans votre cluster, effectuez les opérations suivantes pour chaque nœud du cluster.

Étapes

1. Identifier toutes les LIFs sur un certain nœud.
2. Lancer la commande suivante pour chaque LIF sur le nœud :

   ```
   fcp initiator show -fields wwpn, lif
   ```

   Le nombre d'entrées affichées au bas de la sortie de la commande représente votre nombre d'ITN pour cette LIF.

3. Notez le nombre de moustiquaires imprégnées d'insecticide affichées pour chaque LIF.
4. Ajoutez le nombre de moustiquaires imprégnées d'insecticide pour chaque LIF sur chaque nœud de votre cluster.

   Ce total représente le nombre d'ITN dans votre cluster.

Déterminez si votre cluster peut prendre en charge davantage d'hôtes iSCSI

Le nombre d'hôtes pouvant être connectés directement à un nœud ou qui peuvent être connectés via un ou plusieurs commutateurs dépend du nombre de ports Ethernet disponibles. Le nombre de ports Ethernet disponibles est déterminé par le modèle du contrôleur et par le nombre et le type d'adaptateurs installés dans le contrôleur. Le nombre de ports Ethernet pris en charge pour les contrôleurs et les adaptateurs est disponible dans *Hardware Universe*.

Pour toutes les configurations de clusters à plusieurs nœuds, vous devez déterminer le nombre de sessions iSCSI par nœud pour savoir si vous pouvez ajouter d'autres hôtes à votre cluster. Tant que le cluster est inférieur au nombre maximal de sessions iSCSI par nœud, vous pouvez continuer à ajouter des hôtes au cluster. Le nombre maximal de sessions iSCSI par nœud varie en fonction des types de contrôleurs du cluster.

Étapes

1. Identifiez tous les groupes de portails cible sur le nœud.
2. Vérifier le nombre de sessions iSCSI pour chaque groupe de portails cible sur le nœud :

   ```
   iscsi session show -tpgroup _tpgroup_
   ```

   Le nombre d'entrées affichées au bas de la sortie de la commande représente le nombre de sessions iSCSI pour ce groupe de portails cible.

3. Notez le nombre de sessions iSCSI affichées pour chaque groupe de portails cible.
4. Ajoutez le nombre de sessions iSCSI pour chaque groupe de portails cible sur le nœud.

   Le total représente le nombre de sessions iSCSI sur votre nœud.

Limites de configuration et prise en charge des baies SAN 100 % Flash

Les limites de configuration et la prise en charge varient en fonction de la ONTAP version du système ASA.

Les détails les plus récents sur les limites de configuration prises en charge sont disponibles dans "NetApp Hardware Universe".

> Ces limitations s'appliquent aux systèmes ASA. Si vous possédez un système ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 ou ASA C30), consultez "Limites de stockage du système ASA r2" .

Protocoles SAN et nombre de nœuds pris en charge par cluster

Les protocoles SAN pris en charge et le nombre maximum de nœuds par cluster dépendent de votre configuration non MetroCluster ou MetroCluster :

Configurations non MetroCluster

Le tableau suivant présente la prise en charge des protocoles SAN par ASA et le nombre de nœuds pris en charge par cluster dans des configurations non MetroCluster :

Depuis ONTAP…	Protocoles pris en charge	Nombre maximal de nœuds par cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • ISCSI	12
9.7	• FC • ISCSI	2

Configurations MetroCluster IP

Le tableau ci-dessous présente la prise en charge des protocoles SAN par ASA et le nombre de nœuds pris en charge par cluster dans les configurations MetroCluster IP :

Depuis ONTAP…	Protocoles pris en charge	Nombre maximal de nœuds par cluster
9.15.1	• NVMe/TCP	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds
9.12.1	• NVMe/FC	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds
9.9.1	• FC • ISCSI	4 nœuds par cluster dans des configurations IP MetroCluster à 8 nœuds
9.7	• FC • ISCSI	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds

Prise en charge des ports persistants

Depuis la version ONTAP 9.8, les ports persistants sont activés par défaut sur les baies SAN 100 % Flash (ASA) configurées pour utiliser le protocole FC. Les ports persistants sont uniquement disponibles pour FC et

requièrent l'appartenance de zone identifiée par WWPN (World Wide Port Name).

Les ports persistants réduisent l'impact des basculements en créant une LIF « shadow » sur le port physique correspondant du partenaire haute disponibilité. Lorsqu'un nœud est repris, la LIF shadow sur le nœud partenaire assume l'identité du LIF d'origine, y compris le WWPNe. Avant que le chemin d'accès au nœud mis en service ne soit modifié en défectueux, le shadow LIF apparaît sous la forme d'un chemin actif-optimisé vers la pile MPIO hôte, ainsi que de transferts d'E/S. Cela réduit les perturbations d'E/S car l'hôte voit toujours le même nombre de chemins vers la cible, même lors des opérations de basculement de stockage.

Pour les ports persistants, les caractéristiques de port FCP suivantes doivent être identiques dans la paire haute disponibilité :

- Nombre de ports FCP
- Noms des ports FCP
- Vitesses du port FCP
- Segmentation basée sur le WWPN FCP LIF

Si l'une de ces caractéristiques n'est pas identique au sein de la paire HA, le message EMS suivant est généré :

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Pour plus d'informations sur les ports persistants, reportez-vous à la section "Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne".

Limites de configuration des commutateurs FC utilisés avec les systèmes ONTAP

Les commutateurs Fibre Channel ont des limites de configuration maximales, y compris le nombre de connexions prises en charge par port, groupe de ports, lame et commutateur. Les fournisseurs des commutateurs documentent leurs limites prises en charge.

Chaque interface logique FC (LIF) se connecte à un port de commutateur FC. Le nombre total de connexions à partir d'une seule cible sur le nœud est égal au nombre de LIF plus une connexion pour le port physique sous-jacent. Ne dépassez pas les limites de configuration du fournisseur du commutateur pour les connexions ou d'autres valeurs de configuration. Cela est également vrai pour les initiateurs utilisés côté hôte dans les environnements virtualisés avec NPIV activé. Ne dépassez pas les limites de configuration du fournisseur pour les connexions pour la cible ou les initiateurs utilisés dans la solution.

Limites des commutateurs Brocade

Les limites de configuration des commutateurs Brocade sont indiquées dans les *directives d'évolutivité Brocade*.

Limites du commutateur Cisco Systems

Les limites de configuration des commutateurs Cisco sont disponibles dans le "Limites de configuration Cisco" Guide de la version du logiciel du commutateur Cisco.

Nombre maximal de sauts FC et FCoE pris en charge dans ONTAP

Le nombre de sauts est défini comme le nombre de commutateurs dans le chemin entre

l'initiateur (hôte) et la cible (système de stockage). Le nombre maximal de sauts FC pris en charge entre un hôte et un système de stockage varie en fonction du fournisseur du commutateur.

La documentation de Cisco Systems fait également référence à cette valeur comme le *diamètre de la structure SAN*.

Pour le protocole FCoE, vous pouvez avoir connecté les commutateurs FCoE aux commutateurs FC. Pour les connexions FCoE de bout en bout, les commutateurs FCoE doivent exécuter une version de firmware qui prend en charge les liaisons ISL (Ethernet Inter-switch Links).

Changer de fournisseur	Nombre de sauts pris en charge
Brocade	• 7 pour FC • 5 pour la FCoE
Cisco	• 7 pour FC • Il est possible d'utiliser jusqu'à 3 commutateurs FCoE.

Calculer la profondeur de file d'attente pour les hôtes ONTAP FC

Vous devrez peut-être ajuster la profondeur de votre file d'attente FC sur l'hôte pour obtenir le maximum de valeurs pour les ITN par nœud et le « Fan-In » du port FC. Le nombre maximal de LUN et le nombre de HBA pouvant se connecter à un port FC sont limités par la profondeur de file d'attente disponible sur les ports FC target.

Description de la tâche

La longueur de la file d'attente correspond au nombre de demandes d'E/S (commandes SCSI) pouvant être mises en file d'attente simultanément sur un contrôleur de stockage. Chaque demande d'E/S provenant de l'adaptateur HBA initiateur de l'hôte vers l'adaptateur cible du contrôleur de stockage utilise une entrée de file d'attente. Généralement, une longueur de file d'attente plus élevée équivaut à des performances supérieures. Toutefois, si la profondeur maximale de file d'attente du contrôleur de stockage est atteinte, ce contrôleur de stockage rejette les commandes entrantes en leur renvoyant une réponse QFULL. Si un grand nombre d'hôtes accèdent à un contrôleur de stockage, prévoyez-vous d'éviter les conditions de QFULL qui dégradent considérablement les performances du système et peuvent entraîner des erreurs sur certains systèmes.

Dans une configuration avec plusieurs initiateurs (hôtes), tous les hôtes doivent avoir des profondeurs de file d'attente similaires. En raison des inégalités de profondeur de file d'attente entre les hôtes connectés au contrôleur de stockage via le même port cible, les hôtes dont la profondeur de file d'attente est réduite sont privés d'accès aux ressources par les hôtes dont la profondeur de file d'attente est supérieure.

Les recommandations générales suivantes peuvent être formulées sur les profondeurs de file d'attente « réglage » :

- Pour les systèmes de petite ou moyenne taille, utilisez une longueur de file d'attente HBA de 32.
- Pour les systèmes de grande taille, utilisez une profondeur de file d'attente HBA de 128.
- Pour les cas d'exception ou les tests de performances, utilisez une file d'attente de 256 afin d'éviter tout problème de mise en file d'attente.

- Toutes les profondeurs de file d'attente doivent être définies sur des valeurs similaires pour donner un accès égal à tous les hôtes.
- Pour éviter des pénalités ou des erreurs, la profondeur de la file d'attente du port FC cible du contrôleur de stockage ne doit pas être dépassée.

Étapes

1. Nombre total d'initiateurs FC dans tous les hôtes qui se connectent à un port FC cible.
2. Multiplier par 128.
   - Si le résultat est inférieur à 2,048, définissez la profondeur de la file d'attente pour tous les initiateurs sur 128.
     Vous avez 15 hôtes avec un initiateur connecté à chacun des deux ports cibles du contrôleur de stockage. 15 × 128 = 1,920. Comme 1,920 est inférieur à la limite de profondeur totale de la file d'attente de 2,048, vous pouvez définir la profondeur de la file d'attente pour tous vos initiateurs sur 128.
   - Si le résultat est supérieur à 2,048, passer à l'étape 3.
     Vous avez 30 hôtes avec un initiateur connecté à chacun des deux ports cibles du contrôleur de stockage. 30 × 128 = 3,840. Comme 3,840 est supérieur à la limite de profondeur totale de la file d'attente de 2,048, vous devez choisir l'une des options de l'étape 3 pour résoudre le problème.
3. Choisissez l'une des options suivantes pour ajouter d'autres hôtes au contrôleur de stockage.
   - Option 1 :
     i. Ajoutez d'autres ports FC target.
     ii. Redistribuez vos initiateurs FC.
     iii. Répétez les étapes 1 et 2.

     La profondeur de file d'attente souhaitée de 3,840 dépasse la profondeur de file d'attente disponible par port. Pour y remédier, vous pouvez ajouter un adaptateur cible FC à deux ports à chaque contrôleur puis resegmenter vos commutateurs FC de sorte que 15 de vos 30 hôtes se connectent à un ensemble de ports, et les 15 hôtes restants se connectent à un second ensemble de ports. La profondeur de file d'attente par port est alors réduite à 15 × 128 = 1,920.
   - Option 2 :
     i. Désigner chaque hôte comme « grand » ou « centre commercial » en fonction de ses besoins d'E/S prévus.
     ii. Multiplier le nombre d'initiateurs volumineux par 128.
     iii. Multiplier le nombre de petits initiateurs par 32.
     iv. Additionnez les deux résultats.
     v. Si le résultat est inférieur à 2,048, définissez la profondeur de la file d'attente pour les hôtes volumineux sur 128 et la profondeur de la file d'attente pour les petits hôtes sur 32.
     vi. Si le résultat est toujours supérieur à 2,048 par port, réduisez la profondeur de file d'attente par initiateur jusqu'à ce que la profondeur totale de la file d'attente soit inférieure ou égale à 2,048.

> Pour estimer la profondeur de file d'attente nécessaire pour obtenir un certain débit d'E/S par seconde, utilisez la formule suivante :
>
> Profondeur de file d'attente nécessaire = (nombre d'E/S par seconde) × (temps de réponse)
>
> Par exemple, si vous avez besoin de 40,000 E/S par seconde avec un temps de réponse de 3 millisecondes, la profondeur de file d'attente requise = 40,000 × (.003) = 120.

Le nombre maximal d'hôtes que vous pouvez connecter à un port cible est de 64, si vous décidez de limiter la profondeur de la file d'attente à la recommandation de base de 32. Cependant, si vous décidez d'avoir une profondeur de file d'attente de 128, vous pouvez avoir un maximum de 16 hôtes connectés à un port cible. Plus la longueur de la file d'attente est importante, plus le nombre d'hôtes qu'un seul port cible peut prendre en charge est élevé. Si vous avez besoin de telle sorte que vous ne puissiez pas compromettre la profondeur de la file d'attente, vous devriez obtenir plus de ports cibles.

La profondeur de file d'attente souhaitée de 3,840 dépasse la profondeur de file d'attente disponible par port. Vous disposez de 10 hôtes « grands » qui ont des besoins en E/S de stockage élevés, et de 20 hôtes « petits » qui ont des besoins en E/S faibles. Définissez la profondeur de la file d'attente d'initiateur sur les hôtes volumineux sur 128 et la profondeur de la file d'attente d'initiateur sur les petits hôtes sur 32.

La profondeur totale de file d'attente obtenue est de (10 × 128) + (20 × 32) = 1,920.

Vous pouvez répartir la profondeur de file d'attente disponible de manière égale sur chaque initiateur.

La profondeur de file d'attente par initiateur obtenue est de 2,048 ÷ 30 = 68.

Modifier les profondeurs de file d'attente pour les hôtes SAN ONTAP

Vous devrez peut-être modifier les profondeurs de file d'attente sur votre hôte pour obtenir les valeurs maximales pour les ITN par nœud et le fan-in de port FC. Vous pouvez le faire pour votre environnement."calculer la profondeur de file d'attente optimale"

Hôtes AIX

Vous pouvez modifier la profondeur de la file d'attente sur les hôtes AIX à l'aide de l' `chdev` commande. Modifications effectuées à l'aide du `chdev` la commande persiste entre les redémarrages.

Exemples :

- Pour modifier la profondeur de la file d'attente pour le périphérique hdisk7, utilisez la commande suivante :

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Pour modifier la profondeur de la file d'attente pour l'adaptateur HBA fcs0, utilisez la commande suivante :

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  Valeur par défaut pour `num_cmd_elems` est 200. La valeur maximale est 2,048.

> Il peut être nécessaire de mettre l'adaptateur HBA hors ligne pour le modifier `num_cmd_elems` puis le remettre en ligne à l'aide de `rmdev -l fcs0 -R` et `makdev -l fcs0 -P` commandes.

Hôtes HP-UX

Vous pouvez modifier la profondeur de la file d'attente des LUN ou des périphériques sur les hôtes HP-UX à l'aide du paramètre noyau `scsi_max_qdepth`. Vous pouvez modifier la profondeur de la file d'attente HBA à l'aide du paramètre du noyau `max_fcp_reqs`.

- Valeur par défaut pour `scsi_max_qdepth` est 8. La valeur maximale est 255.

  `scsi_max_qdepth` peut être modifié de manière dynamique sur un système en cours d'exécution à l'aide du `-u` sur le `kmtune` commande. Ce changement sera effectif pour tous les périphériques du système. Par exemple, utilisez la commande suivante pour augmenter la profondeur de la file d'attente de LUN à 64 :

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  Il est possible de modifier la profondeur de la file d'attente pour les fichiers de périphériques individuels à l'aide de l' `scsictl` commande. Modifications à l'aide du `scsictl` les commandes ne sont pas conservées d'un redémarrage système à l'autre. Pour afficher et modifier la profondeur de la file d'attente d'un fichier de périphérique particulier, exécutez la commande suivante :

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- Valeur par défaut pour `max_fcp_reqs` est 512. La valeur maximale est 1024.

  Le noyau doit être reconstruit et le système doit être redémarré pour que les modifications soient apportées à `max_fcp_reqs` pour prendre effet. Pour modifier la profondeur de la file d'attente HBA sur 256, par exemple, utilisez la commande suivante :

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Hôtes Solaris

Vous pouvez définir la profondeur de la file d'attente des LUN et HBA pour vos hôtes Solaris.

- Pour la profondeur de la file d'attente de LUN : le nombre de LUN utilisées sur un hôte multiplié par le papillon par LUN (lun-queue-depth) doit être inférieur ou égal à la valeur tgt-queue-depth sur l'hôte.
- Pour la profondeur de file d'attente dans une pile Sun : les pilotes natifs ne permettent pas pour chaque LUN ou par cible `max_throttle` Paramètres au niveau de la carte HBA. La méthode recommandée pour le réglage du `max_throttle` La valeur pour les pilotes natifs est sur un niveau par type de périphérique (VID_PID) dans l' `/kernel/drv/sd.conf` et `/kernel/drv/ssd.conf` fichiers. L'utilitaire hôte définit cette valeur sur 64 pour les configurations MPxIO et sur 8 pour les configurations Veritas DMP.

Étapes

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`

3. Recherchez `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   La valeur par défaut est 32 lors de l'installation.

4. Définissez la valeur souhaitée en fonction de la configuration de votre environnement.
5. Enregistrez le fichier.
6. Redémarrez l'hôte à l'aide de `sync; sync; sync; reboot -- -r` commande.

Hôtes VMware pour un HBA QLogic

Utilisez le `esxcfg-module` Commande permettant de modifier les paramètres de délai d'expiration de l'adaptateur HBA. Mise à jour manuelle du `esx.conf` le fichier n'est pas recommandé.

Étapes

1. Connectez-vous à la console de service en tant qu'utilisateur root.
2. Utilisez le `#vmkload_mod -l` Commande pour vérifier quel module HBA Qlogic est actuellement chargé.
3. Pour une seule instance d'un HBA Qlogic, exécutez la commande suivante :

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   Cet exemple utilise le module qla2300_707. Utilisez le module approprié en fonction de la sortie de `vmkload_mod -l`.

4. Enregistrez vos modifications à l'aide de la commande suivante :

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. Redémarrez le serveur à l'aide de la commande suivante :

   ```
   #reboot
   ```

6. Vérifiez les modifications à l'aide des commandes suivantes :
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Hôtes VMware pour une carte HBA Emulex

Utilisez le `esxcfg-module` Commande permettant de modifier les paramètres de délai d'expiration de l'adaptateur HBA. Mise à jour manuelle du `esx.conf` le fichier n'est pas recommandé.

Étapes

1. Connectez-vous à la console de service en tant qu'utilisateur root.
2. Utilisez le `#vmkload_mod -l grep lpfc` Commande pour vérifier quelle carte HBA Emulex est actuellement chargée.
3. Pour une seule instance d'un HBA Emulex, entrez la commande suivante :

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

> Selon le modèle de l'adaptateur HBA, le module peut être lpfcdd_7xx ou lpfcdd_732. La commande ci-dessus utilise le module lpfcdd_7xx. Vous devez utiliser le module approprié en fonction des résultats de `vmkload_mod -l`.

L'exécution de cette commande permet de définir la profondeur de la file d'attente de LUN sur 16 pour l'adaptateur HBA représenté par lpfc0.

4. Pour plusieurs instances d'un HBA Emulex, exécutez la commande suivante :

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   La profondeur de la file d'attente LUN pour lpfc0 et la profondeur de la file d'attente LUN pour lpfc1 est définie sur 16.

5. Saisissez la commande suivante :

   ```
   #esxcfg-boot -b
   ```

6. Redémarrez avec `#reboot`.

Hôtes Windows pour une carte HBA Emulex

Sur les hôtes Windows, vous pouvez utiliser `LPUTILNT` Utilitaire de mise à jour de la profondeur de la file d'attente pour les HBA Emulex.

Étapes

1. Exécutez le `LPUTILNT` utilitaire situé dans le `C:\WINNT\system32` répertoire.
2. Sélectionnez **Paramètres de conduite** dans le menu à droite.
3. Faites défiler vers le bas et double-cliquez sur **QueueDepth**.

> Si vous définissez **QueueDepth** supérieur à 150, la valeur suivante du Registre Windows doit également être augmentée de façon appropriée :
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Hôtes Windows pour un HBA Qlogic

Sur les hôtes Windows, vous pouvez utiliser l' et l' `SANsurfer` Utilitaire HBA Manager pour mettre à jour les profondeurs de file d'attente pour les HBA Qlogic.

Étapes

1. Exécutez le `SANsurfer` Utilitaire HBA Manager.
2. Cliquez sur **Port HBA** > **Paramètres**.
3. Cliquez sur **Paramètres avancés du port HBA** dans la zone de liste.
4. Mettez à jour le `Execution Throttle` paramètre.

Hôtes Linux pour HBA Emulex

Vous pouvez mettre à jour les profondeurs de file d'attente d'une carte HBA Emulex sur un hôte Linux. Pour que les mises à jour soient conservées entre les redémarrages, vous devez ensuite créer une nouvelle image de disque RAM et redémarrer l'hôte.

Étapes

1. Identifiez les paramètres de profondeur de file d'attente à modifier :

   ```
   modinfo lpfc|grep queue_depth
   ```

   La liste des paramètres de profondeur de file d'attente avec leur description s'affiche. Selon la version de votre système d'exploitation, vous pouvez modifier un ou plusieurs des paramètres de profondeur de file d'attente suivants :

   - `lpfc_lun_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente vers une LUN spécifique (uint)
   - `lpfc_hba_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente dans un adaptateur Lpfc HBA (uint)
   - `lpfc_tgt_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente sur un port cible spécifique (uint)

     Le `lpfc_tgt_queue_depth` Ce paramètre est uniquement applicable aux systèmes Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11 SP4 et 12.x.

2. Mettez à jour les profondeurs de file d'attente en ajoutant les paramètres de profondeur de file d'attente au `/etc/modprobe.conf` Fichier pour un système Red Hat Enterprise Linux 5.x et vers `/etc/modprobe.d/scsi.conf` Fichier pour un système Red Hat Enterprise Linux 6.x ou 7.x, ou un système SUSE Linux Enterprise Server 11.x ou 12.x.

   Selon la version de votre système d'exploitation, vous pouvez ajouter une ou plusieurs des commandes suivantes :

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Créez une nouvelle image de disque RAM, puis redémarrez l'hôte pour que les mises à jour soient conservées entre les redémarrages.

   Pour plus d'informations, reportez-vous à la section "Administration du système" Pour votre version du système d'exploitation Linux.

4. Vérifiez que les valeurs de profondeur de file d'attente sont mises à jour pour chaque paramètre de profondeur de file d'attente modifié :

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   La valeur actuelle de la profondeur de la file d'attente s'affiche.

Hôtes Linux pour QLogic HBA

Vous pouvez mettre à jour la longueur de la file d'attente d'un pilote QLogic sur un hôte Linux. Pour que les mises à jour soient conservées entre les redémarrages, vous devez ensuite créer une nouvelle image de disque RAM et redémarrer l'hôte. Vous pouvez utiliser l'interface graphique de gestion du HBA QLogic ou l'interface de ligne de commande pour modifier la profondeur de la file d'attente HBA QLogic.

Cette tâche montre comment utiliser la CLI QLogic HBA pour modifier la profondeur de la file d'attente HBA QLogic

Étapes

1. Identifiez le paramètre de profondeur de file d'attente de périphérique à modifier :

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Vous pouvez modifier uniquement le `ql2xmaxqdepth` Paramètre de profondeur de file d'attente, qui indique la profondeur maximale de file d'attente pouvant être définie pour chaque LUN. La valeur par défaut est 64 pour RHEL 7.5 et versions ultérieures. La valeur par défaut est 32 pour RHEL 7.4 et les versions antérieures.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. Mettre à jour la valeur de profondeur de la file d'attente du périphérique :

   - Pour que les modifications persistent, procédez comme suit :

     i. Mettez à jour les profondeurs de file d'attente en ajoutant le paramètre de profondeur de file d'attente au `/etc/modprobe.conf` Fichier pour un système Red Hat Enterprise Linux 5.x et vers `/etc/modprobe.d/scsi.conf` Fichier pour un système Red Hat Enterprise Linux 6.x ou 7.x, ou un système SUSE Linux Enterprise Server 11.x ou 12.x : `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. Créez une nouvelle image de disque RAM, puis redémarrez l'hôte pour que les mises à jour soient conservées entre les redémarrages.

     Pour plus d'informations, reportez-vous à la section "Administration du système" Pour votre version du système d'exploitation Linux.

   - Si vous souhaitez modifier le paramètre uniquement pour la session en cours, exécutez la commande suivante :

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     Dans l'exemple suivant, la profondeur de la file d'attente est définie sur 128.

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. Vérifiez que les valeurs de profondeur de la file d'attente sont mises à jour :

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

La valeur actuelle de la profondeur de la file d'attente s'affiche.

4. Modifiez la profondeur de la file d'attente HBA QLogic en mettant à jour le paramètre de micrologiciel `Execution Throttle` Du BIOS HBA QLogic.

   a. Connectez-vous à l'interface de ligne de commande de gestion QLogic HBA :

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. Dans le menu principal, sélectionnez `Adapter Configuration` option.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

   c. Dans la liste des paramètres de configuration de l'adaptateur, sélectionner le `HBA Parameters` option.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Dans la liste des ports HBA, sélectionnez le port HBA requis.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

Les détails du port HBA s'affichent.

e. Dans le menu Paramètres HBA, sélectionner `Display HBA Parameters` option permettant d'afficher la valeur actuelle de l' `Execution Throttle` option.

La valeur par défaut du `Execution Throttle` option 65535.

```
HBA Parameters Menu

=========================================================
HBA            : 2 Port: 1
SN             : BFD1524C78510
HBA Model      : QLE2562
HBA Desc.      : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version     : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=========================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
---------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
---------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Appuyez sur **entrée** pour continuer.

b. Dans le menu Paramètres HBA, sélectionner `Configure HBA Parameters` Option permettant de modifier les paramètres HBA.

c. Dans le menu configurer les paramètres, sélectionner `Execute Throttle` et mettez à jour la valeur de ce paramètre.

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Appuyez sur **entrée** pour continuer.

e. Dans le menu configurer les paramètres, sélectionner `Commit Changes` option pour enregistrer les

modifications.

f. Quitter le menu.

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.