Référence de configuration SAN

ONTAP 9

NetApp
September 12, 2024

Sommaire

Référence de configuration SAN . . . 1
Présentation de la configuration SAN . . . 1
Configurations iSCSI . . . 1
Configurations FC . . . 4
Configurations FCoE . . . 18
Segmentation Fibre Channel et FCoE . . . 22
Conditions requises pour les configurations SAN partagées . . . 27
Configurations SAN dans un environnement MetroCluster . . . 27
Prise en charge des chemins d’accès multiples sur l’hôte . . . 30
Limites de configuration . . . 31

Référence de configuration SAN

Présentation de la configuration SAN

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

Manières de configurer les hôtes SAN iSCSI

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.

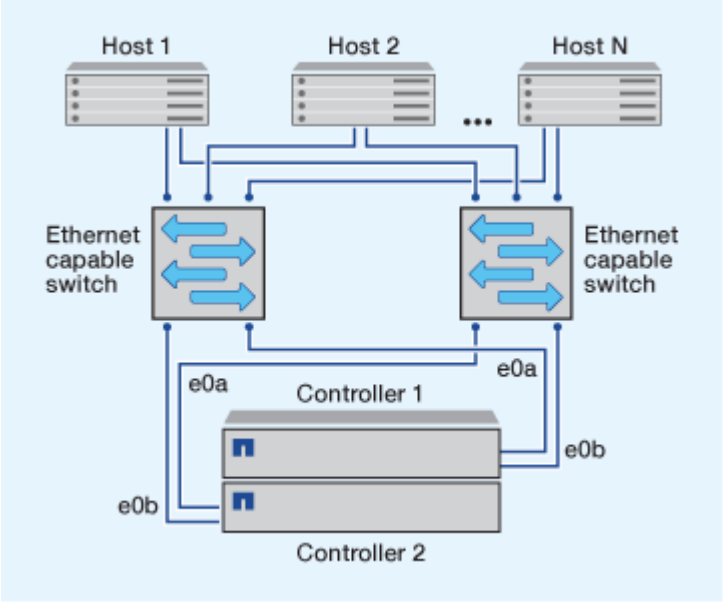
> "Configurations à un seul nœud" ne sont pas recommandées, car elles n'offrent pas la redondance nécessaire à la prise en charge de la tolérance aux pannes et de la continuité de l'activité.

Informations associées

- Découvrez comment "Mappage de LUN sélectif (SLM)" Limite les chemins utilisés pour accéder aux LUN appartenant à une paire HA.
- Découvrez "LIF SAN".
- Découvrez le "Avantages des VLAN dans iSCSI".

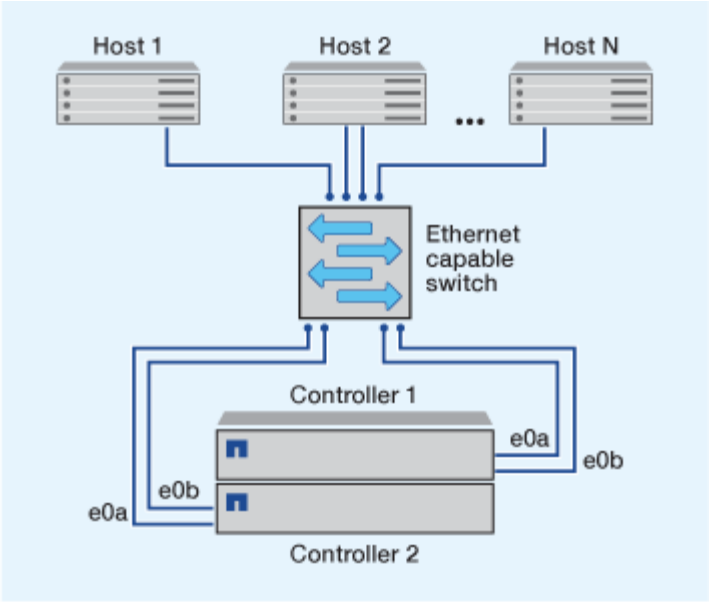
Configurations iSCSI multi-réseau

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.



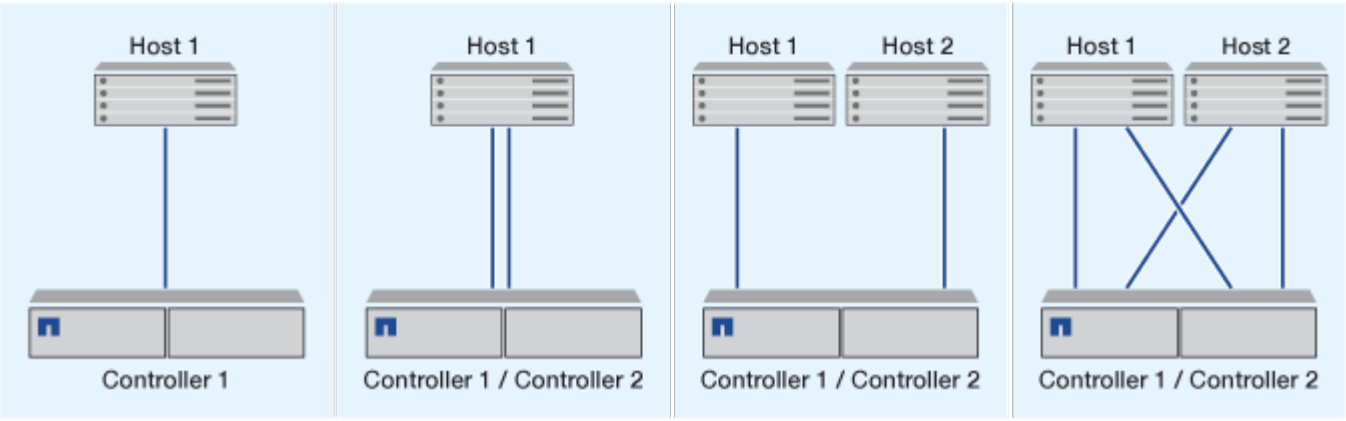
Configurations iSCSI à réseau unique

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 des VLAN dans les 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

Manières de configurer les hôtes SAN FC et FC-NVMe

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.

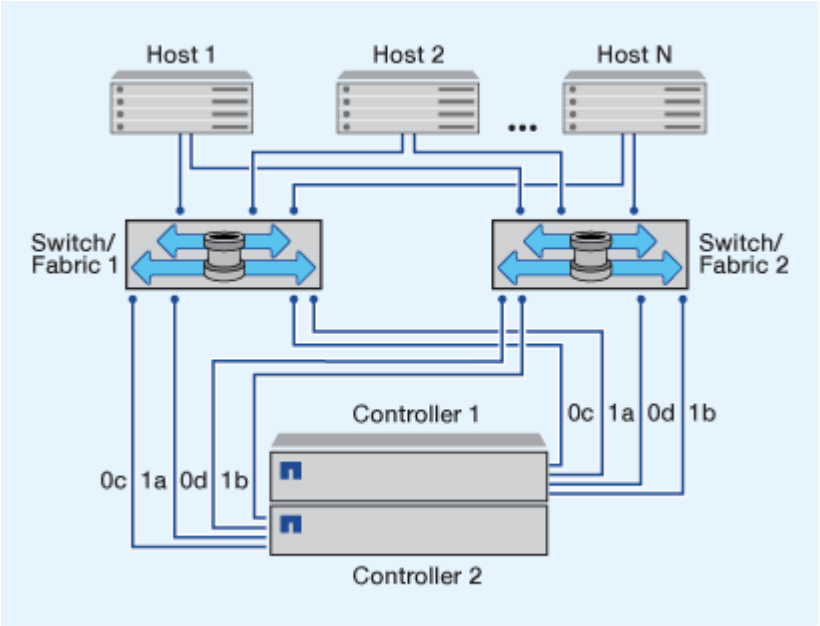
Plusieurs hôtes, qui utilisent différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder aux contrôleurs de stockage en même temps. Les hôtes nécessitent l'installation et la configuration

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.

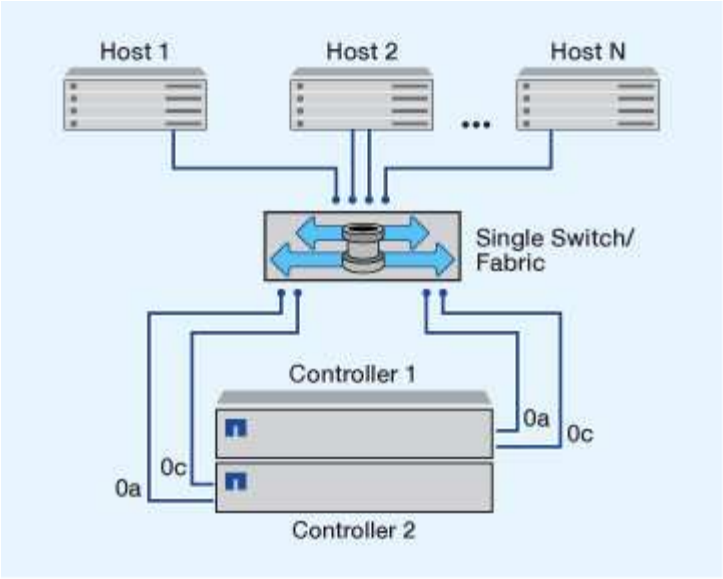


Les configurations FC et FC-NVMe à structure unique

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)" Limite les chemins utilisés pour accéder aux LUN appartenant à une paire HA.
- Découvrez "LIF SAN".

Meilleures pratiques en matière de configuration des commutateurs FC

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 relatives à FC et à l'iSCSI, reportez-vous à "Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne".

Nombre de sauts FC pris en charge

Le nombre maximal de sauts FC pris en charge entre un hôte et un système de stockage dépend du fournisseur du commutateur et de la prise en charge du système de stockage pour les configurations FC.

Le nombre de sauts est défini comme le nombre de commutateurs dans le chemin entre l'initiateur (hôte) et la cible (système de stockage). Cisco désigne également cette valeur par l'expression *diamètre de la structure SAN*.

Changer de fournisseur	Nombre de sauts pris en charge
Brocade	7 pour FC, 5 pour FCoE
Cisco	7 pour FC, jusqu'à 3 commutateurs peuvent être des commutateurs FCoE.

Informations associées

"Téléchargements NetApp : documents Brocade relatifs à la matrice d'évolutivité"

"Téléchargements NetApp : documents Cisco scalabilité Matrix"

Vitesses prises en charge par le port FC cible

Les ports cibles FC peuvent être configurés pour s'exécuter à différentes vitesses. Vous devez définir la vitesse du port cible en fonction de la vitesse du périphérique auquel il se connecte. Tous les ports cibles utilisés par un hôte donné doivent être définis sur la même vitesse.

Les ports cibles FC peuvent être utilisés pour les configurations FC-NVMe de la même manière qu'ils sont utilisés pour les configurations FC.

Vous devez définir la vitesse du port cible afin qu'elle corresponde à la vitesse du périphérique auquel il 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.

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

Les ports UTA2 peuvent utiliser un adaptateur SFP+ de 8 Gb pour prendre en charge les vitesses de 8, 4 et 2 Go, si nécessaire.

Recommandations pour la configuration des ports FC cibles

Pour des performances optimales et une disponibilité optimale, vous devez utiliser la configuration de port cible FC recommandée.

Le tableau suivant indique l'ordre d'utilisation des ports préféré pour les ports intégrés FC et FC-NVMe cibles.

Pour les adaptateurs d'extension, les ports FC doivent être répartis de manière à ne pas utiliser le même ASIC pour la connectivité. L'ordre de slot préféré est indiqué dans le "NetApp Hardware Universe" Pour la version du logiciel ONTAP utilisée par votre contrôleur.

La connectivité FC-NVMe est prise en charge sur les modèles suivants :

- AFF A300

> Les ports intégrés des systèmes AFF A300 ne prennent pas en charge FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800

> Les systèmes FAS2520 ne disposent pas de ports FC intégrés et ne prennent pas en charge les adaptateurs add-on.

Contrôleur	Paires de ports avec ASIC partagé	Nombre de ports cibles : ports préférés
FAS9000, AFF A700, AFF A700S ET AFF A800	Aucune	Tous les ports de données se trouvent sur des adaptateurs d'extension. Voir "NetApp Hardware Universe" pour en savoir plus.
8080, 8060 et 8040	0e+0f 0g+0h	1 : 0e 2 : 0e, 0g 3 : 0e, 0g, 0h 4 : 0e, 0g, 0f, 0h
FAS8200 ET AFF A300	0g+0h	1: 0g 2: 0g, 0h
8020	0c+0d	1 : 0c 2 : 0c, 0d
62xx	0a+0b 0c+0d	1 : 0a 2 : 0a, 0c 3 : 0a, 0c, 0b 4 : 0a, 0c, 0b, 0d

Contrôleur	Paires de ports avec ASIC partagé	Nombre de ports cibles : ports préférés
32xx	0c+0d	1 : 0c 2 : 0c, 0d
FAS2554, FAS2552, FAS2600 SERIES, FAS2720, FAS2750, AFF A200 ET AFF A220	0c+0d 0e+0f	1 : 0c 2 : 0c, 0e 3 : 0c, 0e, 0d 4 : 0c, 0e, 0d, 0f

Gestion des systèmes avec les adaptateurs FC

Présentation de la gestion des systèmes avec des 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 pouvant être configurés en tant qu'initiateurs ou cibles. Vous pouvez également utiliser des cartes d'adaptateur FC configurées en tant qu'initiateurs ou cibles. Les initiateurs se connectent aux tiroirs disques internes, voire aux baies de stockage étrangères (FlexArray). Les cibles se connectent uniquement aux commutateurs FC. Les ports HBA FC cible et la vitesse du port du commutateur doivent être définis sur la même valeur et ne doivent pas être définis sur auto.

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`

Les fonctions que vous recherchez…	Utilisez cette commande…
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`

Configurer les adaptateurs FC pour le mode initiateur

Vous pouvez configurer des ports FC individuels des adaptateurs intégrés et certaines cartes d'adaptateur FC pour le mode initiateur. Ce mode permet de connecter les ports aux lecteurs de bande, aux librairies de bandes ou aux systèmes de stockage tiers à l'aide de FlexArray Virtualization ou Foreign LUN Import (FLI).

Ce dont vous avez besoin

- 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.

Description de la tâche

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 des adaptateurs pouvant être configurés pour le mode cible est disponible dans "NetApp Hardware Universe".

> 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

Vous pouvez configurer des ports FC individuels des adaptateurs intégrés et certaines cartes d'adaptateur FC pour le mode cible. Le mode cible est utilisé pour connecter les ports aux initiateurs FC.

Description de la tâche

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".

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.

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`

Affiche des informations relatives à un adaptateur cible FC

Vous pouvez utiliser le `network fcp adapter show` Commande permettant d'afficher les informations de configuration du système et d'adaptateur pour tout adaptateur FC dans le système.

Étape

1. Affiche des informations relatives à l'adaptateur FC en utilisant le `network fcp adapter show` commande.

   Le résultat de cette commande affiche des informations de configuration du système et des informations sur l'adaptateur pour chaque slot utilisé.

   `network fcp adapter show -instance -node node1 -adapter 0a`

Modifier la vitesse de l'adaptateur FC

Vous devez définir la vitesse du port cible de votre adaptateur afin qu'elle corresponde à la vitesse du périphérique auquel il 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.

Ce dont vous avez besoin

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

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.

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
   ```

Ports FC pris en charge

Le nombre de ports FC intégrés et de ports CNA/UTA2 configurés pour FC varie en fonction du modèle du contrôleur. Les ports FC sont également disponibles par le biais d'adaptateurs d'extension FC cible pris en charge ou de cartes UTA2 supplémentaires configurées avec des adaptateurs FC SFP+.

Ports intégrés FC, UTA et UTA2

- Les ports intégrés peuvent être configurés individuellement en tant que ports FC cible ou initiateur.
- Le nombre de ports FC intégrés diffère selon le modèle de contrôleur.

  Le "NetApp Hardware Universe" Contient la liste complète des ports FC intégrés sur chaque modèle de contrôleur.

- Les systèmes FAS2520 ne prennent pas en charge le protocole FC.

Ports FC des adaptateurs d'extension cibles

- Les adaptateurs d'extension cibles disponibles varient en fonction du modèle de contrôleur.

Le "NetApp Hardware Universe" contient une liste complète des adaptateurs d'extension cibles pour chaque modèle de contrôleur.

- Les ports de certains adaptateurs d'extension FC sont configurés en tant qu'initiateurs ou cibles en usine et ne peuvent pas être modifiés.

  D'autres peuvent être configurés individuellement en tant que ports FC cible ou initiateur, comme les ports FC intégrés. Une liste complète est disponible dans "NetApp Hardware Universe".

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 adaptateurs X1143A-R6

Présentation des configurations de ports prises en charge pour les adaptateurs X1143A-R6

Par défaut, l'adaptateur X1143A-R6 est configuré en mode cible FC, mais vous pouvez configurer ses ports sous forme de ports Ethernet 10 Gb et FCoE (CNA) ou sous forme de ports d'initiateur FC 16 Gb ou cible. Cela nécessite différents adaptateurs SFP+.

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. Les paires de ports connectées au même ASIC doivent être configurées dans le même mode.

En mode FC, l'adaptateur X1143A-R6 se comporte comme tout périphérique FC existant, avec des vitesses pouvant atteindre 16 Gbit/s. En mode CNA, vous pouvez utiliser l'adaptateur X1143A-R6 pour gérer simultanément le trafic NIC et FCoE et partager le même port 10 GbE. Le mode CNA ne prend en charge que le mode FC target pour la fonction FCoE.

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.

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.

   - 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
```

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.

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+ pris en charge et les câbles Twinax (Cisco) sont répertoriés dans le "NetApp Hardware Universe".

Afficher les paramètres de la carte

Pour afficher les paramètres de votre adaptateur cible unifié (X1143A-R6), vous devez exécuter le `system hardware unified-connect show` commande permettant d'afficher tous les modules de votre contrôleur.

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.

Configurations FCoE

Présentation des manières de configurer FCoE

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.

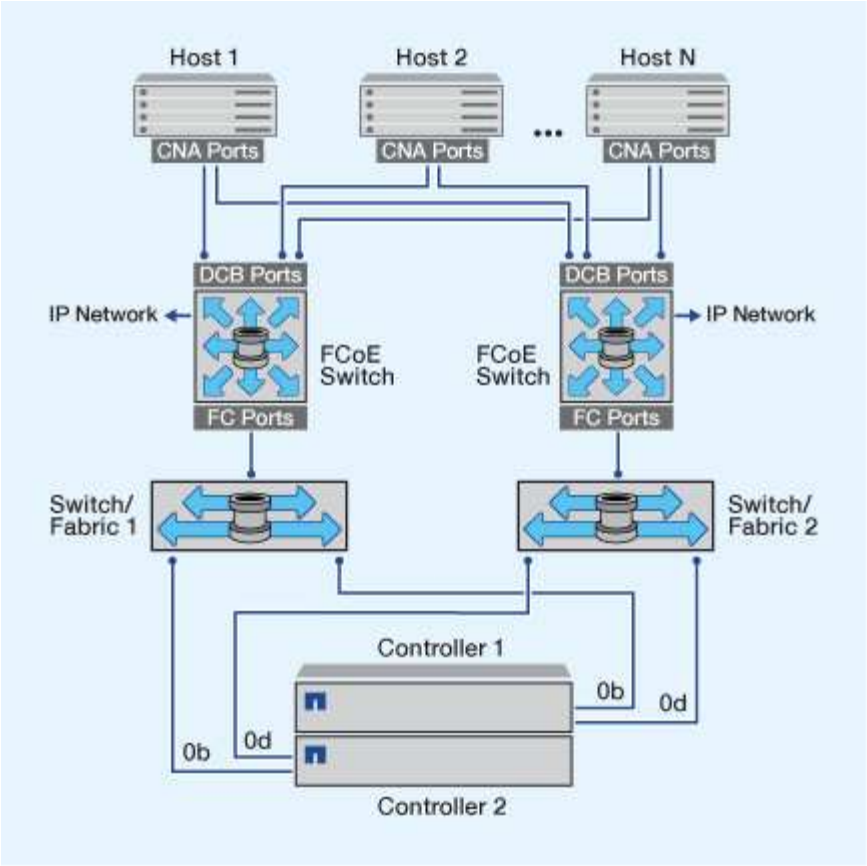
Les configurations FCoE requièrent des commutateurs Ethernet qui prennent explicitement en charge les fonctionnalités FCoE. Les configurations FCoE sont validées par le biais du même processus d'interopérabilité et d'assurance qualité que les commutateurs FC. Les configurations prises en charge sont 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

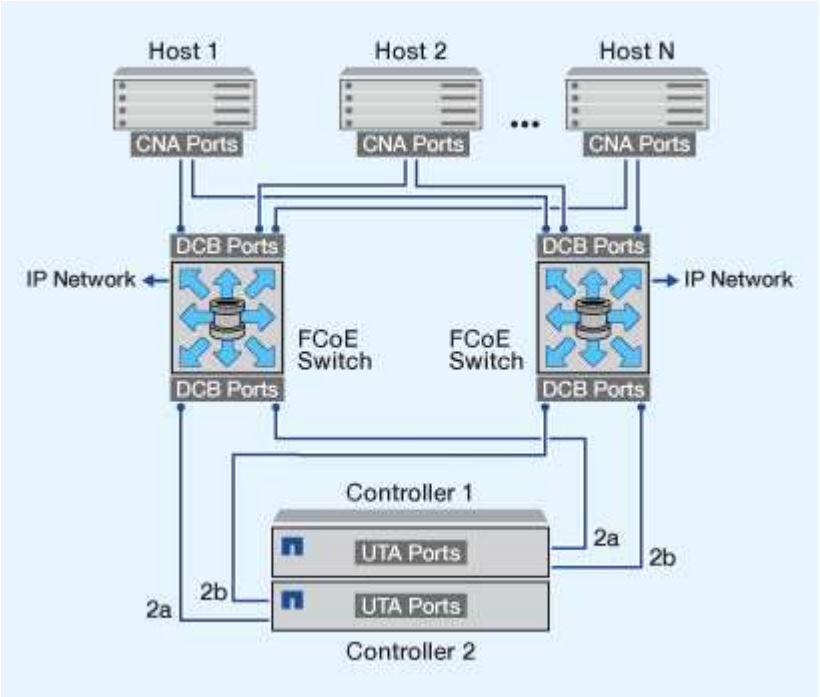
En utilisant les initiateurs FCoE (CNA), vous pouvez connecter des hôtes aux deux contrôleurs d'une paire haute disponibilité via des commutateurs FCoE vers les ports cible FC. Le commutateur FCoE doit également posséder des ports FC. L'initiateur FCoE hôte se connecte toujours au commutateur FCoE. Le 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 :



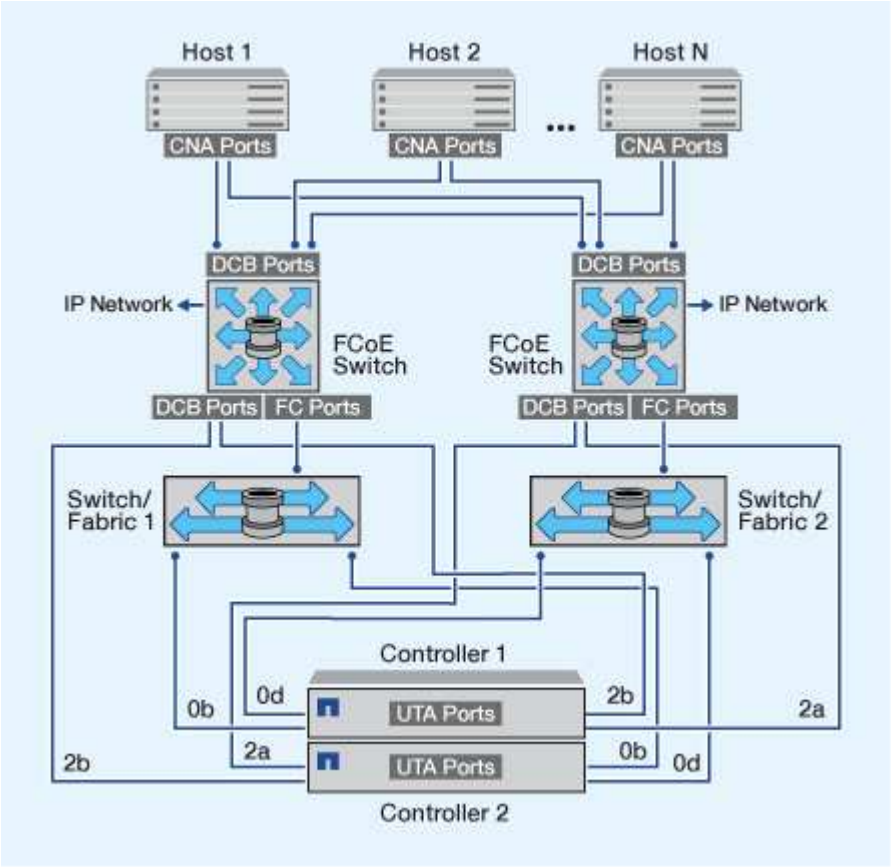
Initiateur FCoE vers la cible FCoE

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.



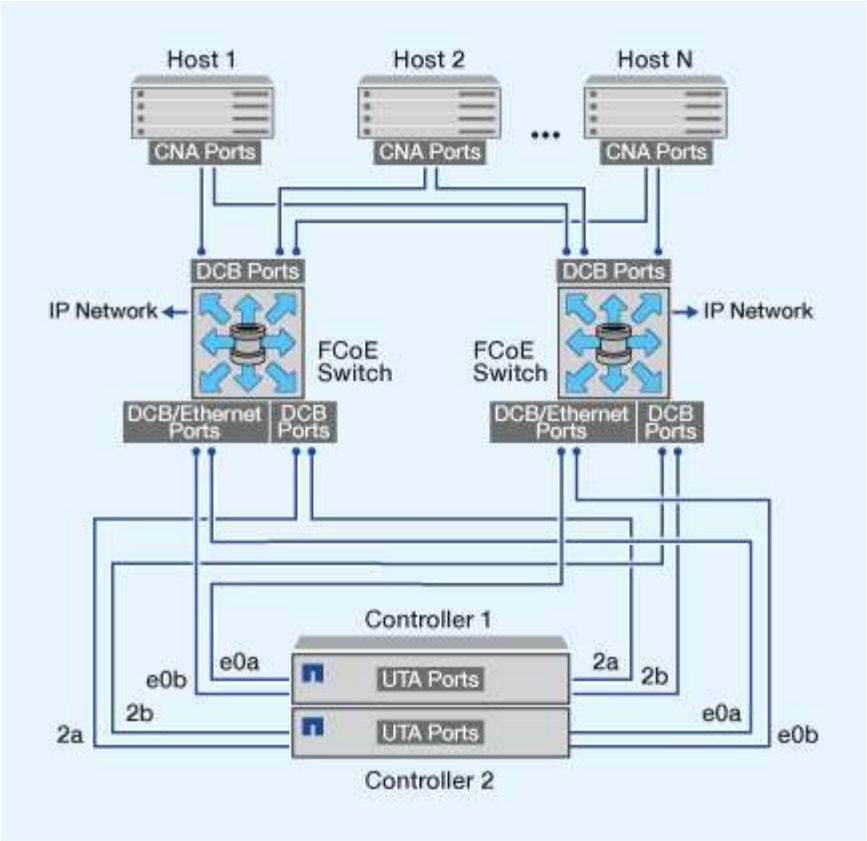
Initiateur FCoE sur les cibles FCoE et FC

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.



Combinaisons d’initiateurs et de cibles 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.

Nombre de sauts pris en charge par FCoE

Le nombre maximal de sauts Fibre Channel over Ethernet (FCoE) pris en charge entre un hôte et un système de stockage dépend du fournisseur du commutateur et de la prise en charge du système de stockage pour les configurations FCoE.

Le nombre de sauts est défini comme le nombre de commutateurs dans le chemin entre l'initiateur (hôte) et la cible (système de stockage). 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).

Le tableau suivant répertorie le nombre maximal de sauts pris en charge :

Changer de fournisseur	Nombre de sauts pris en charge
Brocade	7 pour FC 5 pour la FCoE
Cisco	7 Il est possible d'utiliser jusqu'à 3 commutateurs FCoE.

Segmentation Fibre Channel et FCoE

Présentation de la segmentation Fibre Channel et FCoE

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 avoir une zone commune. La segmentation à un seul initiateur est recommandée.

Motifs de la segmentation

- La segmentation réduit ou élimine la *diaphonie* entre les HBA initiateurs.

Cela se produit même dans les petits environnements et est l'un des meilleurs arguments pour la mise en œuvre du zonage. Les sous-ensembles logiques de structure créés par la segmentation éliminent les problèmes de diaphonie.

- La segmentation réduit le nombre de chemins disponibles vers un port FC, FC-NVMe ou FCoE spécifique. Elle diminue le nombre de chemins entre un hôte et une LUN précise visible.

  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 qu'un pilote de chemins d'accès multiples du système d'exploitation voit. Si une solution de chemins d'accès multiples n'est pas installée sur un hôte, vérifiez qu'un seul chemin d'accès à une LUN est visible en utilisant le zoning dans la structure ou une combinaison de mappage de LUN sélectif (SLM) et de jeux de ports dans le SVM.

- Le zonage renforce la sécurité en limitant l'accès et la connectivité aux points de terminaison qui partagent une zone commune.

  Les ports qui n'ont pas de zones en commun ne peuvent pas communiquer entre eux.

- La segmentation améliore la fiabilité du SAN en isolant les problèmes et réduit le temps de résolution des problèmes en limitant l'espace disponible.

Recommandations pour la segmentation

- Vous devez implémenter le zoning à tout moment si quatre hôtes ou plus sont connectés à un SAN ou si SLM n'est pas implémenté sur les nœuds vers un SAN.
- Bien que la segmentation WWNN (World Wide Node Name) soit possible avec certains fournisseurs de commutateurs, la segmentation WWPN (World Wide Port Name) est nécessaire pour définir correctement un port spécifique et pour utiliser NPIV efficacement.
- La taille de la zone doit être limitée tout en maintenant la facilité de gestion.

  Pour limiter la taille, vous pouvez faire se chevaucher plusieurs zones. En principe, une zone est définie pour chaque hôte ou cluster hôte.

- Vous devez utiliser la segmentation à un seul initiateur pour éliminer la diaphonie entre les HBA initiateurs.

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. Lors de la segmentation dans ONTAP, vous devez utiliser la segmentation WWPN (World Wide Port Name).

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.

Pour les chemins Fibre Channel vers les contrôleurs de stockage qui exécutent ONTAP, assurez-vous que les commutateurs FC sont zonés à l'aide des WWPN des interfaces logiques cibles (LIF), et non pas des WWPN des ports physiques du nœud. Pour plus d'informations sur les LIF, reportez-vous au *ONTAP Network Management Guide*.

"Gestion du réseau"

Zones individuelles

Dans la configuration de segmentation recommandée, il existe un initiateur hôte par zone. La zone se compose du port hôte et d'une ou plusieurs LIF cible sur les nœuds de stockage qui fournissent l'accès aux LUN jusqu'au nombre souhaité de chemins par cible. Cela signifie que les hôtes accédant aux mêmes nœuds ne peuvent pas voir les ports des autres hôtes, mais que l'initiateur peut accéder à tous les nœuds.

Vous devez ajouter toutes les LIF du serveur virtuel de stockage (SVM) dans 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.

Pour les chemins Fibre Channel vers les nœuds qui exécutent ONTAP, assurez-vous que les commutateurs FC sont zonés à l'aide des WWPN des interfaces logiques cibles (LIF), et non pas des WWPN des ports physiques du nœud. Les WWPN des ports physiques commencent par « 50 » et les WWPN des LIF commencent par « 20 ».

Segmentation à structure unique

Dans une configuration à structure unique, vous pouvez toujours connecter chaque initiateur hôte à chaque nœud de stockage. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples. Chaque hôte doit avoir deux initiateurs pour les chemins d'accès multiples pour fournir la résilience dans la solution.

Chaque initiateur doit disposer d'au moins une LIF à partir de chaque nœud auquel celui-ci 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.

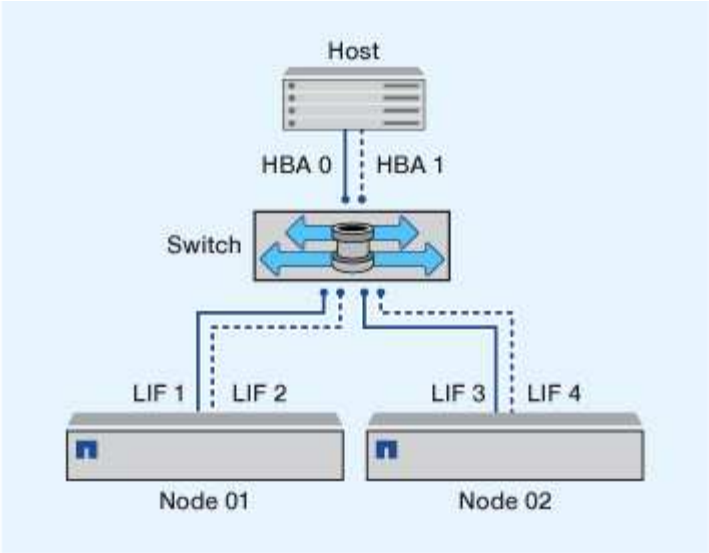
Les configurations à structure unique sont prises en charge, mais ne sont pas considérées comme hautement disponibles. La défaillance d'un seul composant peut entraîner la perte de l'accès aux données.

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 incluait plus de nœuds, les LIF pour les nœuds supplémentaires seraient incluses dans ces zones.



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.

Informations associées

"NetApp Hardware Universe"

Segmentation par paire haute disponibilité à double fabric

Dans les configurations à double structure, vous pouvez connecter chaque initiateur hôte à chaque nœud du cluster. Chaque initiateur hôte utilise un autre commutateur pour accéder aux nœuds du cluster. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples.

Les configurations à double structure sont considérées comme haute disponibilité, car l'accès aux données est maintenu en cas de défaillance d'un composant.

Dans la figure suivante, l'hôte a deux initiateurs et exécute un logiciel de chemins d'accès multiples. Il y a deux zones. SLM est configuré de sorte que tous les nœuds soient considérés comme des nœuds de rapport.

> 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.

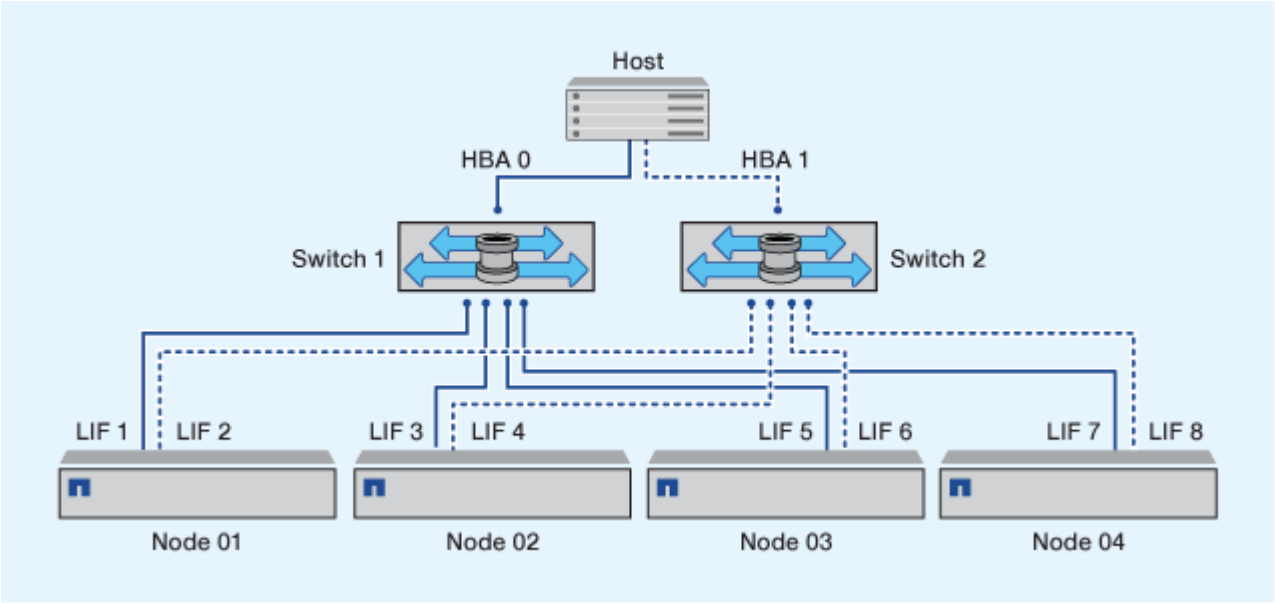
- Zone 1 : HBA 0, LIF_1, LIF_3, LIF_5 et LIF_7
- Zone 2 : HBA 1, LIF_2, LIF_4, LIF_6 et LIF_8

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 initiateur 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 d'une solution en cluster, en fonction du paramètre SLM (Selective LUN Map) et de la configuration de nœud de reporting. 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 incluait plus de nœuds, les LIF pour les nœuds supplémentaires seraient 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.

Informations associées

"NetApp Hardware Universe"

Restrictions de segmentation pour les commutateurs Cisco FC et FCoE

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.

Le protocole FC-NVMe utilise régulièrement des switchs FC de la même manière qu'ils sont utilisés pour le protocole FC.

- Plusieurs LIF pour les protocoles FC et FCoE peuvent partager des ports physiques sur un nœud tant qu'ils se trouvent dans des zones différentes.
- FC-NVMe et FCoE ne peuvent pas partager le même port physique.
- Les protocoles FC et FC-NVMe peuvent partager le même port physique de 32 Go.
- Les commutateurs FC et FCoE Cisco exigent que chaque LIF d'un port donné se trouve dans une zone distincte des autres LIF du port en question.

- Une seule zone peut avoir à la fois des LIF FC et FCoE. Une zone peut contenir une LIF à partir de chaque port cible du cluster, mais veillez à ne pas dépasser les limites de chemin de l'hôte et à vérifier la configuration SLM.
- Les LIF présentes sur différents ports physiques peuvent se trouver dans la même zone.
- Les commutateurs Cisco exigent la séparation des LIF.

  Bien qu'elles ne soient pas requises, la séparation des LIF est recommandée pour tous les commutateurs

Conditions requises pour les configurations SAN partagées

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 dans un environnement 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 entre le basculement et le rétablissement

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 1. 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 des chemins d'accès multiples sur l'hôte

Prise en charge des hôtes pour la présentation des chemins d'accès multiples

ONTAP utilise toujours le protocole ALUA (Asymmetric Logical Unit Access) pour les chemins FC et iSCSI. Veillez à utiliser des configurations hôtes qui prennent en charge ALUA pour les protocoles FC et iSCSI.

Depuis la version ONTAP 9.5, le basculement/rétablissement de paire haute disponibilité multivoie est pris en charge dans les configurations NVMe utilisant un accès asynchrone à l'espace de noms (ANA). Dans ONTAP 9.4, NVMe ne prend en charge qu'un chemin d'accès de l'hôte à la cible. L'hôte applicatif doit gérer le basculement des chemins vers son partenaire haute disponibilité (HA).

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.

Lorsque le logiciel de chemins d'accès multiples de l'hôte est requis

Si il existe plusieurs chemins entre les interfaces logiques (LIF) du SVM et la structure, un logiciel de chemins d'accès multiples est nécessaire. Il est nécessaire de disposer de chemins d'accès multiples sur l'hôte chaque fois que l'hôte peut accéder à une LUN via plusieurs chemins.

Le logiciel de chemins d'accès multiples présente un seul disque au système d'exploitation pour tous les chemins d'accès à une LUN. Sans le logiciel de chemins d'accès multiples, le système d'exploitation pourrait traiter chaque chemin en tant que disque distinct, ce qui peut entraîner une corruption des 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

Le logiciel de chemins d'accès multiples est recommandé dans les configurations haute disponibilité. Outre le mappage sélectif des LUN, il est recommandé d'utiliser des zoning switch FC ou des ensembles de ports pour

limiter les chemins d'accès aux LUN.

Le logiciel de chemins d'accès multiples est également appelé le logiciel MPIO (chemins d'accès E/S multiples).

Nombre recommandé de chemins entre l'hôte et les nœuds dans le cluster

Vous ne devez pas dépasser huit chemins entre votre hôte et chaque nœud du cluster, en tenant compte du nombre total de chemins pouvant être pris en charge pour le système d'exploitation hôte et les chemins d'accès multiples utilisés sur cet hôte.

Au moins deux chemins par LUN doivent être connectés à chaque nœud de reporting via le mappage de LUN sélectif (SLM) utilisé 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

Informations associées

"Administration SAN"

Limites de configuration

Identification du nombre de nœuds pris en charge dans les configurations SAN

Le nombre de nœuds par cluster pris en charge par ONTAP varie en fonction de la version de ONTAP, des modèles de contrôleur de stockage dans le cluster et du protocole de vos nœuds de cluster.

Description de la tâche

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. Cliquez sur **plates-formes** dans le coin supérieur gauche (en regard du bouton **Home**) et sélectionnez le type de plate-forme.
3. Cochez la case en regard de votre version de ONTAP.

Une nouvelle colonne s'affiche pour vous permettre de choisir vos plates-formes.

4. Cochez les cases en regard des plateformes utilisées dans votre solution.
5. Désélectionnez la case **Sélectionner tout** dans la colonne **Choisissez vos spécifications**.
6. Cochez la case **Max Nodes per Cluster (NAS/SAN)**.
7. Cliquez sur **Afficher les résultats**.

Informations associées

"NetApp Hardware Universe"

Détermination du nombre d'hôtes pris en charge par cluster dans les configurations FC et FC-NVMe

Le nombre maximal d'hôtes SAN pouvant être connectés à un cluster varie considérablement en fonction de votre combinaison spécifique de plusieurs attributs de cluster, tels que le nombre d'hôtes connectés à chaque nœud de cluster, les initiateurs par hôte, les sessions par hôte et les nœuds du cluster.

Description de la tâche

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. Tant que vous êtes en dessous du 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.

Identification du nombre d'hôtes pris en charge dans les configurations iSCSI

Le nombre maximal d'hôtes SAN pouvant être connectés dans des configurations iSCSI varie considérablement en fonction de votre combinaison spécifique de plusieurs attributs de cluster, tels que le nombre d'hôtes connectés à chaque nœud de cluster, les initiateurs

par hôte, les connexions par hôte et les nœuds du cluster.

Description de la tâche

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 des commutateurs FC

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.

Calculer la profondeur de la file d’attente

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.

Définissez la profondeur de file d'attente sur les hôtes SAN

Vous devrez peut-être modifier la profondeur des files d'attente sur votre hôte pour atteindre les valeurs maximales pour les ITN par nœud et le Fan-In du port FC.

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.